

the network security company™

Palo Alto Networks®

Protección avanzada del endpoint
Guía del administrador
Versión 3.2

Información de contacto

Sede de la empresa:

Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

Acerca de esta guía

Esta guía describe la instalación inicial y la configuración básica de los componentes de la Protección avanzada del endpoint de Palo Alto Networks, e incluye el Endpoint Security Manager (ESM) y Traps. Los temas incluyen requisitos previos, prácticas recomendadas y procedimientos para la instalación y administración de Traps en los endpoints de su organización.

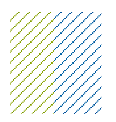
Consulte las siguientes fuentes para obtener más información:

- https://paloaltonetworks.com/documentation: Sitio de documentación de publicaciones técnicas.
- https://live.paloaltonetworks.com: Permite acceder a la base de conocimientos, la documentación al completo, foros de debate y vídeos.
- https://support.paloaltonetworks.com: Aquí podrá contactar con el servicio de asistencia técnica, informarse sobre los programas de asistencia y gestionar su cuenta o sus dispositivos.
- https://support.paloaltonetworks.com/Updates/SoftwareUpdates: Para leer las notas sobre la última versión, vaya a la página de actualizaciones de software en
- Para enviar sus comentarios sobre la documentación, diríjase a: documentation@paloaltonetworks.com

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Fecha de revisión: agosto 26, 2015

Índice



Descripción general de la protección avanzada del endpoint

La protección avanzada del endpoint es una solución que previene amenazas persistentes avanzadas (APT) y ataques de día cero, y habilita la protección de sus endpoints bloqueando vectores de ataque antes de que se inicie el malware.



Para acceder a la versión 3.2 más reciente de la Protección avanzada del endpoint, visite la página Documentación de Protección avanzada del endpoint en el portal de documentación técnica.

Los temas siguientes describen la Protección avanzada del endpoint de forma más detallada:

- Descripción general de la Protección avanzada del endpoint
- Componentes de la protección avanzada del endpoint

Descripción general de la Protección avanzada del endpoint

Los ciberataques se realizan en redes o endpoints para causar daños, robar información o lograr otros objetivos que incluyen la toma de control de los sistemas informáticos que pertenecen a otros. Los adversarios perpetran los ataques haciendo que un usuario ejecute de forma no intencionada un ejecutable malintencionado, o explotando una debilidad en un ejecutable legítimo para ejecutar un código malintencionado sin que el usuario tenga conocimiento de ello.

Una forma de evitar estos ataques es la identificación de ejecutables, librerías de enlace dinámico (DLL), u otras partes del código como malintencionadas y, entonces, evitar su ejecución probando cada módulo de código potencialmente peligroso frente una lista de firmas de amenazas específicas. La debilidad de este método es que las soluciones basadas en firmas necesitan tiempo para identificar las amenazas de nueva creación conocidas solo por el atacante (también denominadas ataques día cero o exploits) y añadirlas a la lista de amenazas conocidas, dejando el endpoint vulnerable hasta que se actualizan las firmas.

La solución de Protección avanzada del endpoint, que consiste en un administrador de seguridad de endpoints (EMS) y el software de protección de endpoints llamado Traps, es más efectiva en la prevención de ataques. En vez de intentar seguir la siempre creciente lista de amenazas conocidas, Traps configura una serie de *obstáculos* que previenen los ataques en sus puntos de entrada inicial, cuando los ejecutables legítimos están a punto de permitir accesos malintencionados al sistema.

Traps se centra en las vulnerabilidades del software en procesos que abren archivos no ejecutables utilizando técnicas de prevención de exploits. Traps también utiliza técnicas de prevención de malware para evitar la ejecución de archivos ejecutables malintencionados. Con este doble enfoque, la solución AEP puede evitar todo tipo de ataques, ya sean amenazas conocidas o desconocidas.

Todos los aspectos de los ajustes de seguridad del endpoint son altamente configurables: los endpoints y los grupos a los que se aplican, las aplicaciones que protegen y las reglas, restricciones y acciones definidas. Esto permite a cada organización configurar Traps a medida de sus necesidades, para obtener la máxima protección con una mínima alteración de sus actividades diarias.

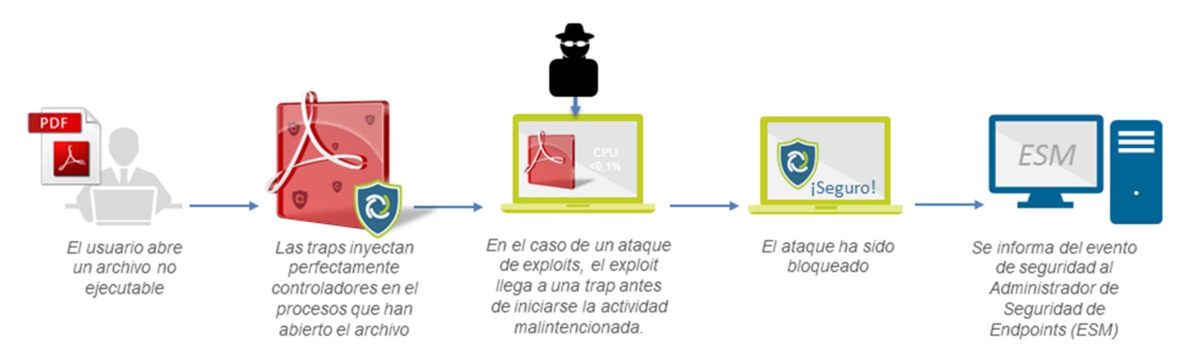
- Prevención de exploits
- Prevención del malware

Prevención de exploits

Un exploit es una secuencia de comandos que aprovecha un bug o vulnerabilidad de una aplicación de software o proceso. Los atacantes utilizan exploits como el medio para acceder y aprovecharse de un sistema. Para obtener el control de un sistema, el atacante debe superar una cadena de vulnerabilidades del sistema. El bloqueo de cualquier intento de ataque de una vulnerabilidad del sistema bloqueará el exploit completamente.

En un ataque típico, el atacante intenta obtener el control de un sistema tratando en primer lugar de corromper o esquivar la asignación de memoria o los gestores de la misma. Utilizando técnicas de corrupción de memoria, como desbordamiento de búfer o corrupción o daños en la pila, el hacker puede entonces activar un bug en el software o explotar una vulnerabilidad de un proceso. A continuación, el atacante debe manipular un programa para que ejecute el código facilitado o especificado por él y evadir la detección. Si el atacante logra acceder al sistema operativo, puede entonces cargar troyanos, programas de malware que contienen ejecutables malintencionados, o usar el sistema de cualquier otro modo para su ventaja.

Traps evita esos intentos de exploit con el uso de obstáculos o trampas en cada etapa del intento de exploit.



Cuando un usuario abre un archivo no ejecutable, por ejemplo, un documento de PDF o Word, el agente de Traps inyecta controladores en el software que abre el archivo. Los controladores se inyectan en la etapa más temprana posible, antes de que se cargue en la memoria cualquier archivo perteneciente al proceso. Si el proceso que abre el archivo está protegido, Traps inyecta un módulo de código denominado *Módulo de prevención de exploits (EPM)* en el proceso. El EPM se dirige a una técnica de exploits específica y se ha diseñado para evitar ataques a las vulnerabilidades de los programas basándose en la corrupción de memoria o fallos lógicos.

Los ejemplo de ataques que pueden evitar los EPM incluyen secuestro de librerías DLL (sustitución de una DLL legítima por una malintencionada con el mismo nombre), suplantación del flujo de control de un programa y la inserción de un código malintencionado como gestor de excepciones.

Además de proteger automáticamente los procesos contra los citados ataques, Traps informa de cualquier evento de prevención al Endpoint Security Manager, y realiza acciones adicionales según los ajustes de las reglas de políticas. Las acciones comunes que realiza Traps incluyen la recopilación de datos forenses y la información al usuario en relación con el evento. Traps no realiza ninguna acción adicional de exploración o monitorizado.

Por defecto, la política de seguridad del endpoint protege las aplicaciones más vulnerables y las que se utilizan con más frecuencia, pero también se pueden añadir a la lista de procesos protegidos otras aplicaciones propias y de terceros. Para obtener más información, consulte Añadir un proceso protegido, provisional o desprotegido.

Para obtener más información, consulte Reglas de protección de exploits.

Prevención del malware

Los archivos ejecutables malintencionados, conocidos como malware o software malintencionado, habitualmente simulan ser archivos no maliciosos o van integrados en ellos. Estos archivos, en ocasiones denominados troyanos, pueden dañar los equipos al intentar obtener el control, al recopilar información confidencial o al interrumpir las operaciones normales del sistema.

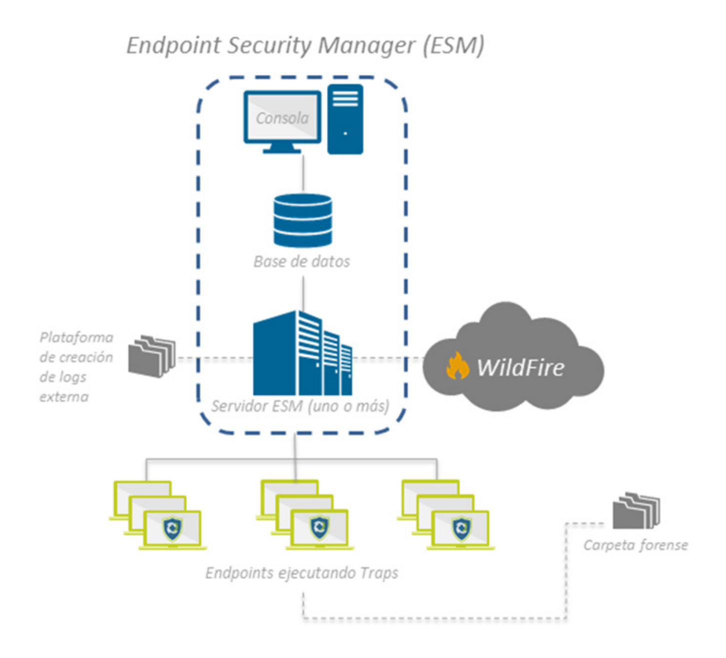
Para proteger los endpoints de archivos ejecutables malintencionados, Traps emplea el *Motor de prevención de malware* como otro tipo de obstáculo de seguridad. El motor de prevención de malware utiliza una combinación de restricciones basadas en las políticas, módulos de prevención de malware y análisis de WildFire para limitar el área superficial de un ataque y controlar la fuente de instalación de archivos, por ejemplo, medios externos. El motor de prevención de malware también utiliza mitigaciones basadas en la técnica que limitan o bloquean procesos secundarios, procesos de Java iniciados en los navegadores web, creación de subprocesos y procesos remotos, y la ejecución de procesos sin firma.

Cuando se produce un evento de seguridad, las acciones comunes realizadas por Traps incluyen la prevención de la ejecución del archivo, recopilación de datos forenses e información al usuario en relación con el evento. Traps no realiza ninguna acción adicional de exploración o monitorizado.

Para obtener más información, consulte Flujo de prevención del malware.

Componentes de la protección avanzada del endpoint

La solución AEP utiliza un Endpoint Security Manager (ESM) central compuesto de una consola ESM, una base de datos y un servidor ESM para administrar las reglas de las políticas, y distribuir la política de seguridad a los endpoints de su organización. Los componentes del Endpoint Security Manager se comunican con el software de protección, denominado Traps, que se instala en cada endpoint de su organización. El diagrama siguiente muestra los componentes de la Protección avanzada del endpoint.



Los temas siguientes describen los elementos de forma más detallada:

- Consola Endpoint Security Manager
- Servidor Endpoint Security Manager
- Base de datos
- Endpoints
- Traps
- Plataforma de logging externa
- WildFire
- Carpeta forense

Consola Endpoint Security Manager

La consola Endpoint Security Manager (ESM) es una interfaz basada en la web que incluye un panel de administración para gestionar los eventos de seguridad, el estado del endpoint y las reglas de las políticas. Se puede instalar la interfaz web en el mismo servidor que el servidor ESM, en un servidor separado o en un servidor en la nube. La consola ESM se comunica con la base de datos de forma independiente del servidor ESM.

Servidor Endpoint Security Manager

Cada servidor Endpoint Security Manager (ESM) funciona como un servidor de conexión que transporta información entre los componentes del ESM, Traps y WildFire. Cada servidor ESM tiene capacidad para hasta 50.000 agentes de Traps. Con regularidad, el servidor ESM recopila la política de seguridad de la base de datos y la distribuye a los agentes de Traps. Cada agente de Traps envía información relacionada con los eventos de seguridad al servidor ESM. La tabla siguiente muestra los tipos de mensajes que el agente de Traps envía al servidor ESM:

Tipo de mensaje	Descripción
Estado de Traps	El agente de Traps envía periódicamente mensajes al servidor ESM para indicar que está operativo, y para solicitar la política de seguridad más reciente. Las páginas de notificaciones y estado del Endpoint Security Manager muestran el estado de cada endpoint. Por defecto, la duración entre mensajes, conocido como periodo heartbeat, es de cinco minutos; el periodo heartbeat es configurable.
Notificaciones	El agente de Traps envía mensajes de notificación sobre los cambios del agente al servidor ESM; por ejemplo, cuándo se inicia o se detiene un servicio. El servidor almacena logs de estas notificaciones en la base de datos. Pueden verse las notificaciones en el Endpoint Security Manager. Por defecto, Traps envía notificaciones cada dos horas.
Actualizar mensajes	Un usuario final puede solicitar una actualización inmediata de las políticas haciendo clic en el botón **Registrar ahora** de la consola de Traps. Esto hace que el agente de Traps solicite la política de seguridad más reciente al servidor ESM sin esperar a que transcurra el periodo heartbeat.
Informes de prevención	Si ocurre un evento de prevención en un endpoint en el que se ha instalado un agente de Traps, el agente envía toda la información relacionada con el evento al servidor ESM en tiempo real.

Base de datos

La base de datos almacena información administrativa, reglas de las políticas de seguridad, historial de los endpoints y otras informaciones sobre eventos de seguridad. La base de datos se gestiona mediante la plataforma MS-SQL. Cada base de datos requiere una licencia y puede comunicarse con uno o más servidores ESM. Las base de datos puede instalarse en el mismo servidor que la consola ESM y el servidor ESM, por ejemplo, en un entorno independiente o puede instalarse en un servidor dedicado.



Durante la etapa de prueba de concepto, también es compatible la base de datos SQLite.

Endpoints

Un endpoint es un equipo, servidor, máquina virtual o dispositivo móvil basado en Windows que ejecuta la aplicación de protección en el lado del cliente denominada Traps. Para conocer los requisitos previos, consulte Requisitos previos para la instalación de Traps en un endpoint.

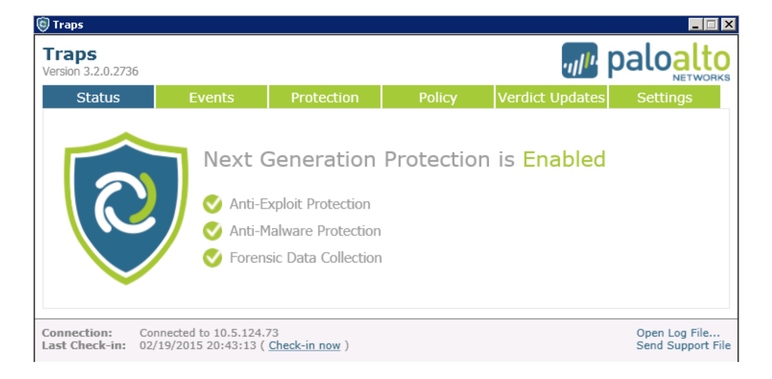
Traps

Traps está compuesto de una consola que incluye una aplicación de interfaz de usuario, un agente que protege el endpoint y se comunica con el servidor ESM y el servicio que obtiene los datos forenses.

El agente de Traps protege el endpoint implementando la política de seguridad definida para la organización en el Endpoint Security Manager. Cuando un usuario crea o abre un proceso protegido en el endpoint, el agente de Traps inyecta sus controladores en el proceso en la etapa más temprana posible, antes de que los archivos del proceso se carguen en la memoria. El agente también protege el software Traps contra su deshabilitación o desinstalación.

Si el agente de Traps encuentra un evento de prevención, el servicio de Traps recopila información forense y transmite los datos relacionados con el evento al Endpoint Security Manager. El servicio de Traps también comunica con regularidad la información del estado del endpoint.

La consola de Traps muestra información acerca de los procesos protegidos, historial de eventos y política de seguridad actual. Normalmente, los usuarios no necesitan ejecutar la consola de Traps, pero la información puede ser de utilidad cuando se investiga un evento relacionado con la seguridad. Se puede decidir ocultar el icono de la bandeja de la consola que activa la consola, o evitar que los usuarios la activen. Para obtener más información, consulte Ocultación o restricción de acceso a la consola de Traps.



Plataforma de logging externa

Al especificar una plataforma de creación de logs externa, es posible obtener una vista agregada de los logs de todos los servidores ESM. El Endpoint Security Manager puede escribir logs en una plataforma de creación de logs externa como, por ejemplo, un sistema SIEM, servicios SOC o syslog, además de almacenar sus propios logs de forma interna. También se puede integrar el servidor syslog con herramientas de monitorizado de terceros, como Splunk, para analizar los datos logs. Descargue al aplicación Splunk para Palo Alto Networks en https://apps.splunk.com/app/491/.

Para añadir una plataforma de logging externa, consulte Habilitar informes utilizando la consola ESM.

WildFire



El agente de Traps se ha diseñado para bloquear ataques antes de que se ejecute cualquier código malintencionado en el endpoint. Aunque este enfoque garantiza la seguridad de los datos y la infraestructura, permite recopilar información forense solamente en el momento de la prevención. De este modo, no puede revelar completamente la finalidad del ataque y su flujo completo.

El servicio WildFire es un sistema opcional de análisis post-prevención que realiza análisis forenses de archivos malintencionados. Al activar la integración del de WildFire, se permite a Traps crear un hash de archivo del archivo ejecutable y comprobarlo en la nube de WildFire o en un aparato WildFire local. Si WildFire confirma que un archivo es malware conocido, el agente de Traps bloquea el archivo para futuras exposiciones e informa al ESM.

Cuando WildFire detecta un nuevo malware, genera nuevas firmas en un plazo de una hora tras la detección. Los cortafuegos de siguiente generación de Palo Alto Networks equipados con una suscripción de WildFire pueden recibir las nuevas firmas en los siguientes 3015 minutos; los cortafuegos con solo una suscripción de Threat Prevention pueden recibir las nuevas firmas en la siguiente actualización de firma del antivirus, en las próximas 24-48 horas.

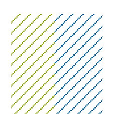
Si se habilita la integración de WildFire en la consola ESM, la página de estado de la consola de Traps muestra un junto a **Recopilación de datos forenses**. Si WildFire no está habilitado, la consola de Traps muestra un junto a **Recopilación de datos forenses**.

Para más información, consulte Habilitación de WildFire y Flujo de prevención del malware.

Carpeta forense

Cuando Traps encuentra un evento relacionado con la seguridad, como una ejecución de un archivo, interferencias con el servicio de Traps, o un ataque de exploits, realiza un log de detalles forenses en tiempo real en relación con el evento del endpoint. Los datos forenses incluyen el historia del evento, volcado de memoria y otras informaciones asociadas con el evento. Puede obtener los datos forenses creando una regla de acción para recopilar los datos del endpoint. Cuando el endpoint recibe la política de seguridad que incluye la regla de acción, el agente de Traps envía toda la información forense a la carpeta forense, a la que en ocasiones se denomina carpeta de cuarentena.

Durante la instalación inicial, se especifica la ruta de la carpeta forense que utiliza el Endpoint Security Manager para almacenar la información forense que recopila de los endpoints. El ESM es compatible con múltiples carpetas forenses en Protección avanzada del endpoint 3.2 o posterior y habilita el Servicio de transferencia inteligente en segundo plano (BITS) en la carpeta durante la instalación. Si no se puede acceder a la carpeta forense especificada durante la instalación, Traps utiliza por defecto la carpeta forense especificada en la consola ESM. Puede cambiar la carpeta por defecto en cualquier momento utilizando el Endpoint Security Manager.



Escenarios de implementación de la Protección avanzada del endpoint

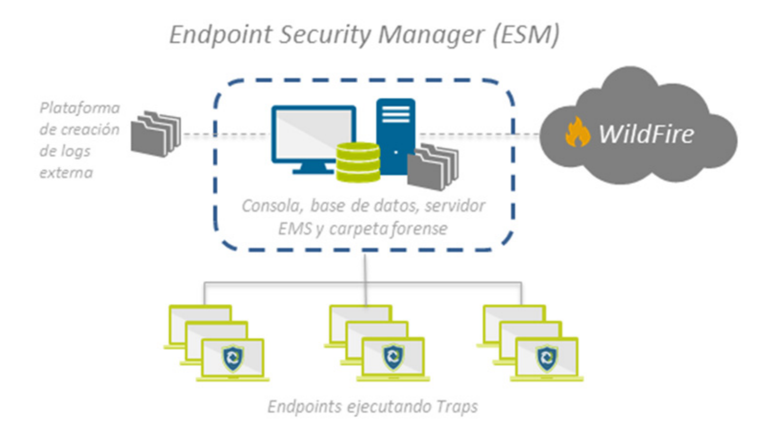
Puede implementar la solución de Protección avanzada del endpoint en una amplia variedad de entornos. Los temas siguientes describen los escenarios típicos de implementación, tomando en consideración el número de agentes y sitios:

- Implementación independiente
- Implementaciones pequeñas
- Implementaciones grandes

Para los requisitos previos y consideraciones en relación con la instalación, consulte Requisitos previos.

Implementación independiente

Componentes de implementación independiente



Para una prueba de concepto (POC) inicial o un sitio pequeño con menos de 250 agentes de Traps, utilice una implementación independiente para instalar los siguientes componentes del Endpoint Security Manager (ESM) en un solo servidor o una máquina virtual:

- Servidor ESM
- Consola ESM
- Carpeta forense (cuarentena)
- Base de datos
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.
- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

Para las prácticas correctas en el uso de un enfoque en fases en la instalación de Traps en endpoints, consulte Etapas de implementación de Traps.

Requisitos para la implementación independiente

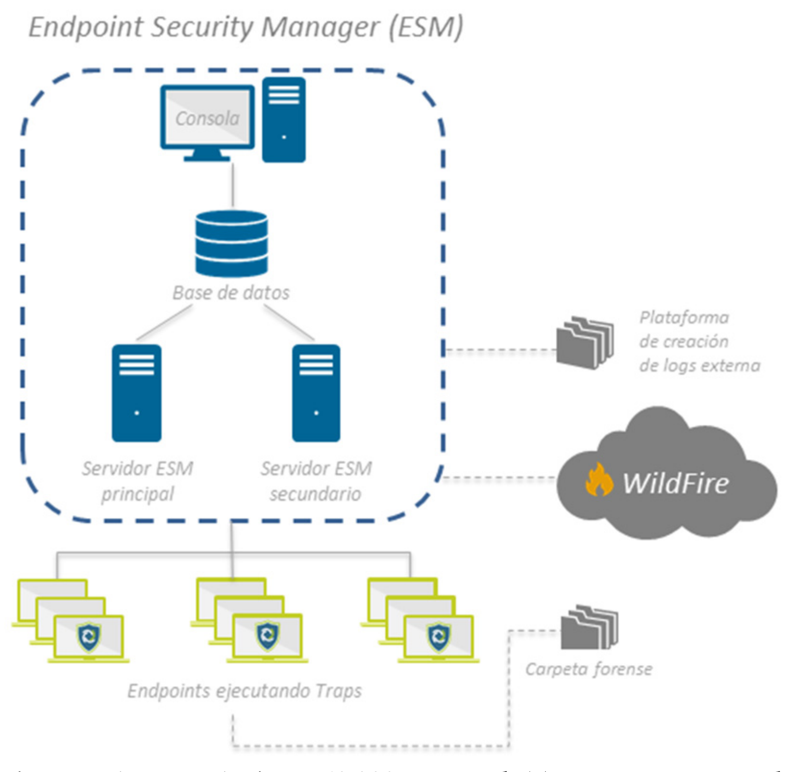
La tabla siguiente muestra los requisitos para un servidor independiente.

Requisito	Valor
Procesador	Pentium 4 y superior
Memoria	512MB de RAM
Espacio en disco	100MB
Aplicación de base de datos	SQLite (solo POC) o MS-SQL

Para los requisitos de Traps, consulte Requisitos previos para la instalación de Traps en un endpoint.

Implementaciones pequeñas

Implementaciones pequeñas de un solo sitio

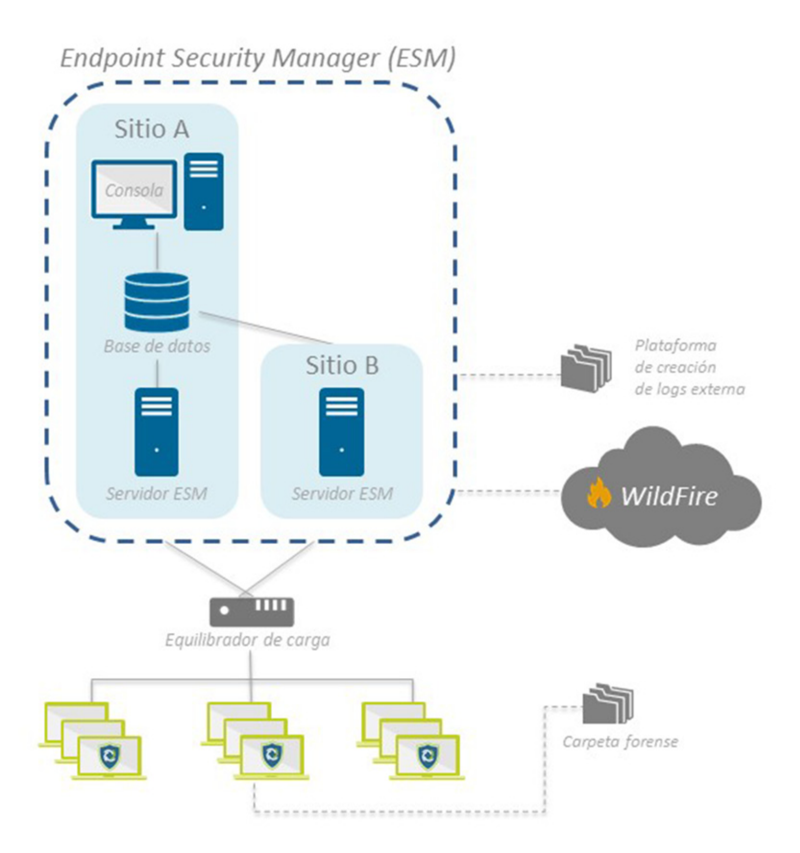


Este escenario de implementación permite hasta 50.000 agentes de Traps en un entorno de un solo sitio y está compuesto de los siguientes componentes:

- Un servidor de base de datos dedicado
- Una consola Endpoint Security Manager (ESM) que ejecute 3.2 para la administración de la política de seguridad y los agentes de Traps
- Dos servidores ESM que ejecuten ESM Core 3.2, uno principal y otro de respaldo, en el mismo segmento de red que el servidor de base de datos y la consola
- Carpeta forense a la que pueden acceder todos los endpoints para guardar en tiempo real los detalles forenses relacionados con eventos de seguridad
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.
- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

En este escenario de implementación, un solo sitio contiene la base de datos, las consola ESM para la administración de las políticas locales y los endpoints y servidores ESM redundantes. Si no se puede acceder al servidor ESM principal, los agentes de Traps se conectan al Endpoint Security Manager utilizando el servidor de respaldo. Ambos servidores obtienen la política de seguridad de la base de datos y la distribuyen a los agentes.

Implementaciones pequeñas de sitios múltiples



Este escenario de implementación permite hasta 100.000 agentes de Traps (5.000 por sitio) en un entorno de sitios múltiples y está compuesto de los siguientes componentes:

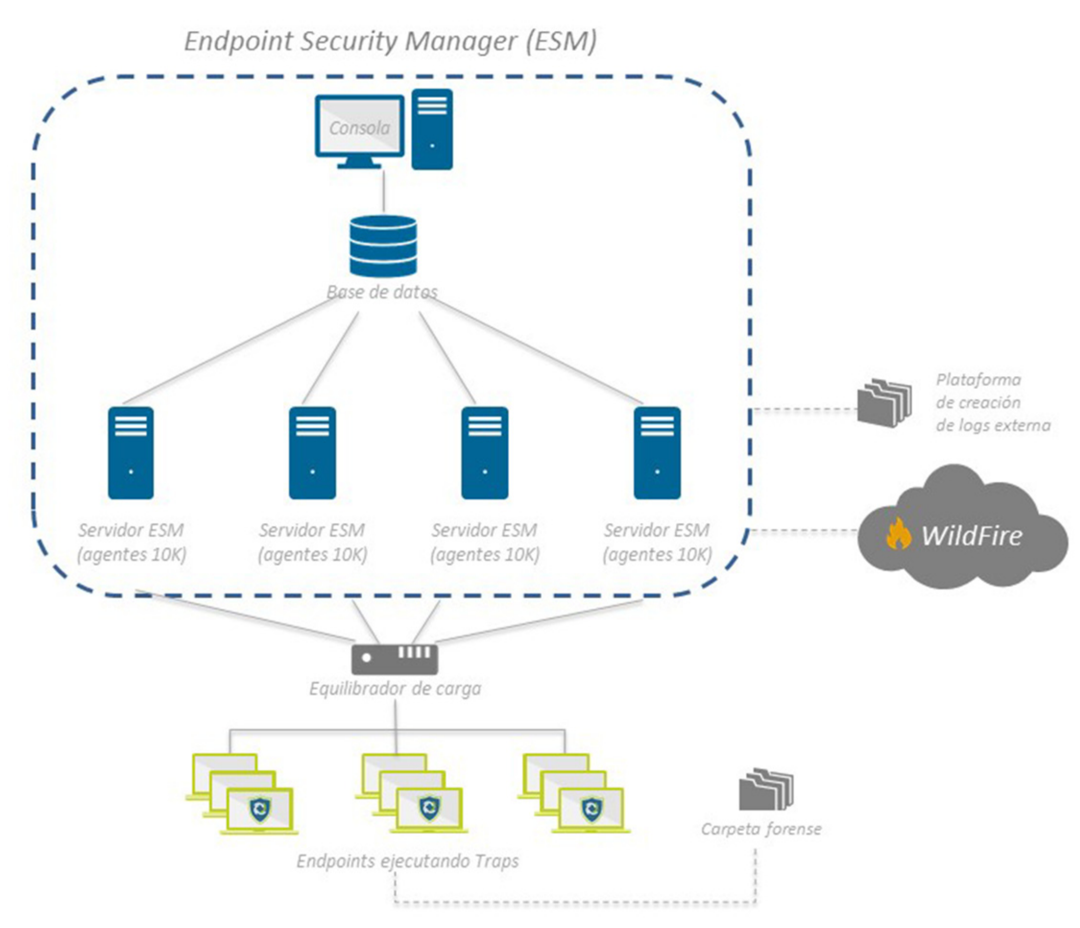
- Una base de datos dedicada en uno de los sitios
- Una consola Endpoint Security Manager (ESM) que ejecuta 3.2 en la misma localización que la base de datos para administrar la política de seguridad y los agentes de Traps
- Un servidor ESM por sitio o dos servidores ESM por sitio para la redundancia, cada uno de ellos ejecutando ESM Core 3.2.
- Carpeta forense a la que pueden acceder todos los endpoints para guardar en tiempo real los detalles forenses relacionados con eventos de seguridad
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.

- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

En este escenario de implementación, el Sitio A contiene un servidor ESM, la base de datos y una consola ESM para la administración de políticas locales y endpoints. El Sitio B contiene un segundo servidor ESM con capacidad para 50.000 agentes adicionales (un total de 100.000 agentes de Traps). Ambos servidores obtienen la política de seguridad de la base de datos localizada en el Sitio A y la distribuyen a los agentes. Los agentes se conectan con el servidor ESM principal de su sitio, mientras el servidor ESM del otro sitio actúa como servidor secundario de respaldo.

Implementaciones grandes

Implementaciones grandes de un solo sitio



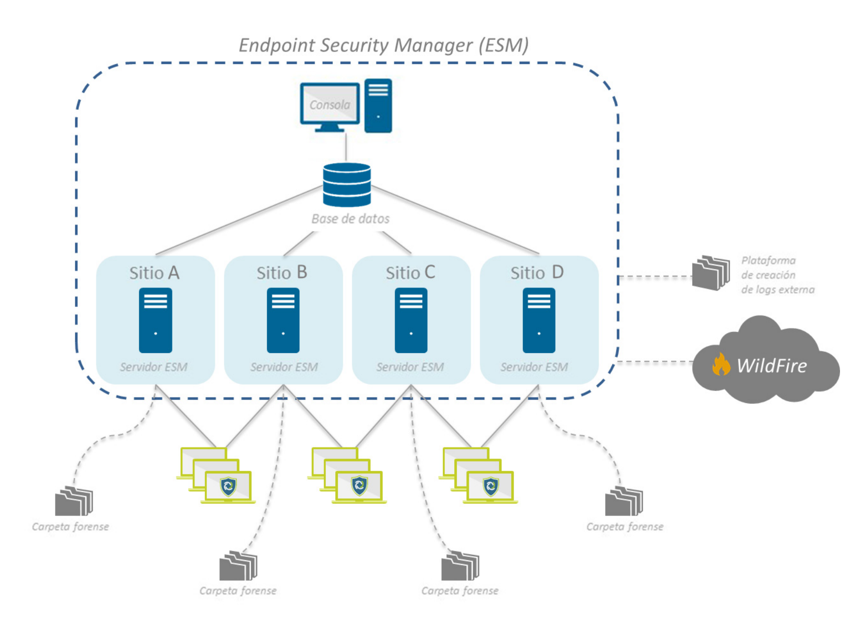
Este escenario de implementación permite hasta 200.000 agentes de Traps (50.000 por sitio) en un entorno de un solo sitio y está compuesto de los siguientes componentes:

- Un servidor de base de datos dedicado
- Una consola Endpoint Security Manager (ESM) que ejecuta 3.2 en la misma localización que la base de datos para administrar la política de seguridad y los agentes de Traps

- Servidores ESM, uno para cada 50.000 agentes de Traps, y cada uno de ellos ejecutando ESM Core 3.2
- Carpeta forense, una por servidor ESM a la que puedan acceder todos los endpoints para guardar en tiempo real los detalles forenses relacionados con eventos de seguridad
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.
- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

En este ejemplo, se puede conectar hasta 200.000 agentes de Traps al Endpoint Security Manager. Para permitir este escenario, los endpoints se conectan a cuatro servidores ESM a través de un equilibrador de carga opcional. Cada servidor ESM se conecta a una base de datos central administrada por una consola ESM dedicada.

Aplicación de sitios múltiples grandes con un Endpoint Security Manager



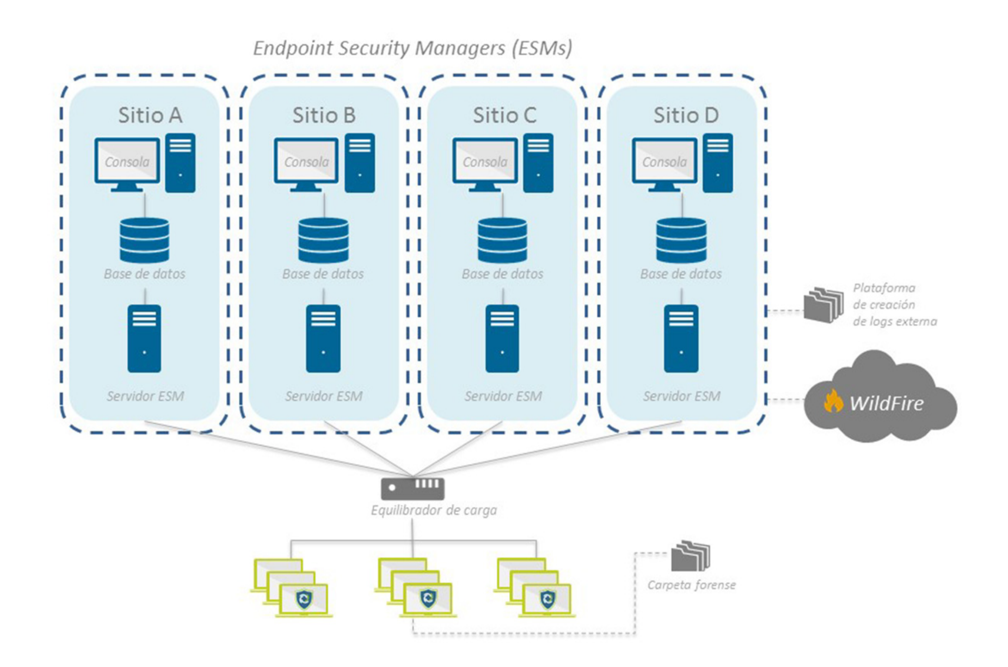
Este escenario de implementación permite hasta 200.000 agentes de Traps (50.000 por sitio) en un entorno de sitios múltiples y está compuesto de los siguientes componentes:

- Un servidor de base de datos dedicado
- Una consola Endpoint Security Manager (ESM) que ejecuta 3.2 en la misma localización que la base de datos para administrar la política de seguridad y los agentes de Traps
- Servidores ESM, uno para cada 50.000 agentes de Traps en cada sitio, y cada uno de ellos ejecutando ESM Core 3.2
- Carpeta forense a la que pueden acceder todos los endpoints para guardar en tiempo real los detalles forenses relacionados con eventos de seguridad
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.

- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

En este ejemplo se asume que cada uno de los sitios A, B, C y D necesita hasta 50.000 agentes de Traps. Para permitir este escenario, cada sitio contiene un servidor ESM que recupera la política de seguridad de la base de datos situada en el Sitio A. Los agentes se conectan al Endpoint Security Manager utilizando sus servidores ESM locales como servidor principal y usan los servidores ESM de otros sitios como servidores secundarios.

Aplicación de sitios múltiples grandes con múltiples Endpoint Security Manager



Este escenario de implementación permite hasta 200.000 agentes de Traps (50.000 por sitio) en un entorno de sitios múltiples y está compuesto de los siguientes componentes:

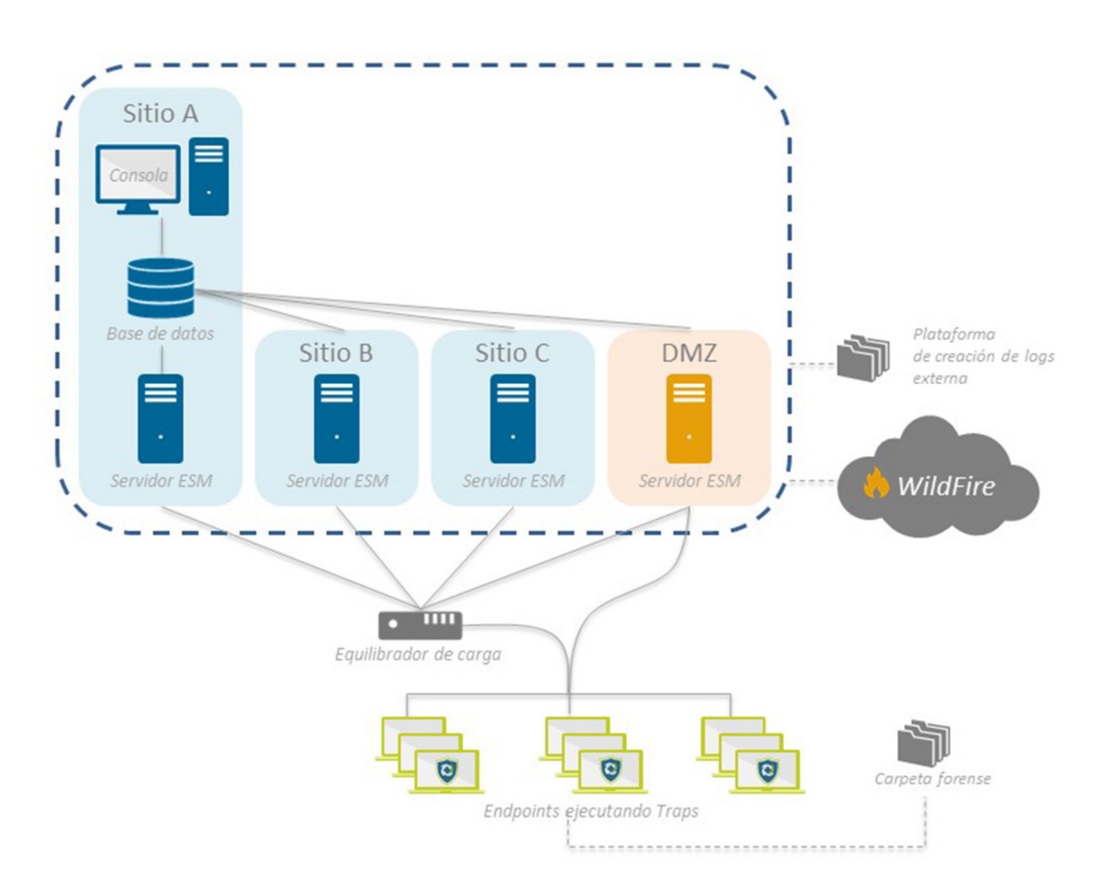
- Un Endpoint Security Manager (ESM), por sitio:
  - Una base de datos dedicada (con licencia)
  - Una consola ESM que ejecuta 3.2 en la misma localización que la base de datos para administrar la política de seguridad y los agentes de Traps
  - Servidores ESM, uno para cada 50.000 agentes de Traps en cada sitio, y cada uno de ellos ejecutando ESM Core 3.2
- Carpeta forense a la que pueden acceder todos los endpoints para guardar en tiempo real los detalles forenses relacionados con eventos de seguridad
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.
- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

En este ejemplo se asume que cada uno de los sitios A, B, C y D necesita hasta 50.000 agentes de Traps. Para permitir este escenario, cada sitio administra políticas de seguridad de forma independiente frente a otros sitios utilizando un Endpoint Security Manager local compuesto de un servidor ESM, una base de datos y una consola ESM. Los agentes se conectan al Endpoint Security Manager utilizando sus servidores ESM locales como servidor principal y utilizan los servidores ESM de otros sitios como servidores secundarios.



No se recomienda el uso de bases de datos en un clúster debido a la posibilidad de colisión entre las bases de datos. En los casos en que ya esté en funcionamiento la solución de bases de datos, configure los agentes de Traps para la utilización de una sola dirección IP virtual (VIP) para acceder al clúster de bases de datos.

Implementación grande de sitios múltiples con agentes en itinerancia (sin VPN)



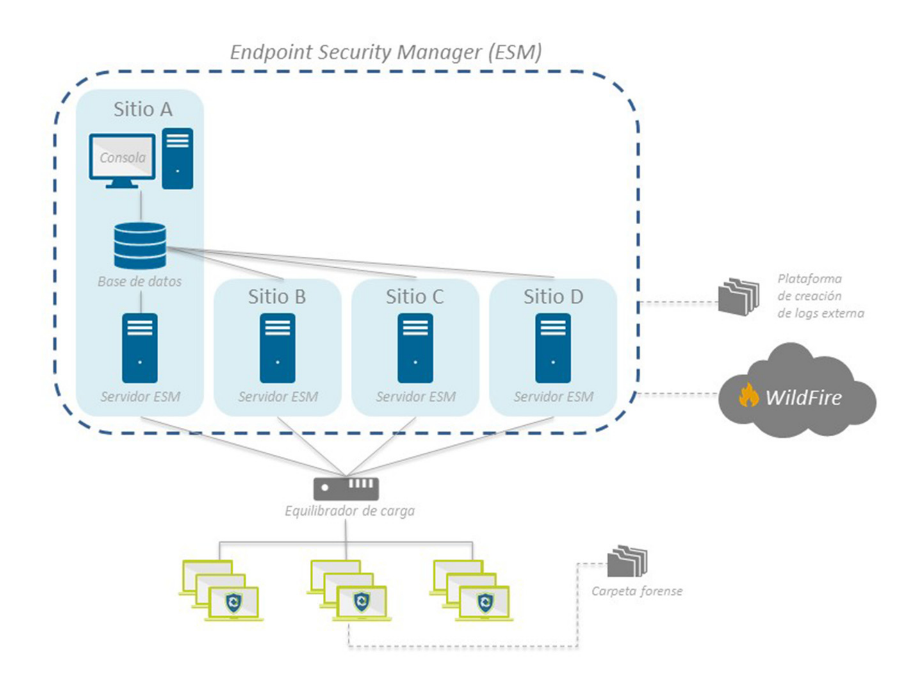
Este escenario de implementación permite hasta 200.000 agentes de Traps (5.000 por sitio) en un entorno de sitios múltiples y está compuesto de los siguientes componentes:

- Un servidor de base de datos dedicado
- Una consola Endpoint Security Manager (ESM) que ejecuta 3.2 en la misma localización que la base de datos para administrar la política de seguridad y los agentes de Traps

- Servidores ESM, uno para cada 50.000 agentes de Traps en cada sitio, y cada uno de ellos ejecutando ESM Core 3.2
- Un servidor ESM con un registro DNS público que acepte las conexiones de agentes de Traps en itinerancia, bien:
  – Un servidor ESM con un puerto configurado para aceptar conexiones de redes externas
  – Un servidor ESM instalado en un DMZ con una conexión al servidor de base de datos interno. Este servidor también puede funcionar como servidor de respaldo secundario.
- Carpeta forense a la que pueden acceder todos los endpoints para guardar en tiempo real los detalles forenses relacionados con eventos de seguridad
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.
- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

En este ejemplo, se asume que los sitios A, B y C requieren hasta 50.000 agentes de Traps cada uno y que 50.000 endpoints están en itinerancia. Para permitir este escenario, cada sitio contiene un servidor ESM que recupera la política de seguridad de la base de datos situada en el Sitio A. Los endpoints internos se conectan al Endpoint Security Manager utilizando sus servidores ESM locales. Los endpoints externos se conectan a través de un servidor ESM público localizado en un DMZ o a través de un puerto que se configura para permitir el tráfico de redes externas. Si un endpoint está en itinerancia y no se puede conectar al servidor ESM, Traps recoge los datos de prevención localmente hasta que el agente puede establecer una conexión con la carpeta forense.

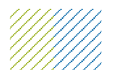
Implementación grande de sitios múltiples con agentes en itinerancia (sin VPN)



Este escenario de implementación permite hasta 200.000 agentes de Traps (50.000 por sitio) que se conectan a través de los sitios locales y localizaciones off-site a través de un túnel VPN. Este entorno de sitios múltiples está compuesto de los componentes siguientes:

- Un servidor de base de datos dedicado
- Una consola Endpoint Security Manager (ESM) que ejecuta 3.2 en la misma localización que la base de datos para administrar la política de seguridad y los agentes de Traps
- Servidores ESM, uno para cada 50.000 agentes de Traps en cada sitio, y cada uno de ellos ejecutando ESM Core 3.2
- Conexión VPN para proporcionar a los usuarios en itinerancia una dirección IP interna para la conexión al servidor ESM.
- Carpeta forense a la que pueden acceder todos los endpoints para guardar en tiempo real los detalles forenses relacionados con eventos de seguridad
- (Opcional) Equilibrador de carga para la distribución del tráfico a través de los servidores EMS.
- (Opcional) Plataforma de logging externa, como un SIEM o syslog
- (Opcional) Integración WildFire

En este ejemplo, se asume que los sitios A, B, C y D requieren hasta 50.000 agentes de Traps cada uno y que algunos de esos agentes pueden estar localizados off-site. Para permitir este escenario, cada sitio contiene un servidor ESM que recupera la política de seguridad de la base de datos situada en el Sitio A. Los endpoints internos se conectan al Endpoint Security Manager utilizando sus servidores ESM locales. Los endpoints externos se conectan a través de un túnel VPN que prorporciona el endpoint con una dirección IP interna para la conexión al sitio. Si un endpoint está en itinerancia y no se puede conectar a través de VPN, Traps recoge los datos de prevención localmente hasta que el agente puede establecer una conexión con la carpeta forense.



Requisitos previos

Los temas siguientes describen los requisitos previos para la instalación de la infraestructura de Traps.

- Requisitos previos para la instalación del servidor ESM
- Requisitos previos para la instalación de Traps en un endpoint

Requisitos previos para la instalación del servidor ESM

Antes de instalar el software de Protección avanzada del endpoint 3.2 en el servidor ESM, asegúrese de que el servidor cumple con los siguientes requisitos previos:

- ESM Core y la consola ESM ejecutándose en la misma versión de la Protección avanzada del endpoint.
- 300 MB de espacio libre en disco más espacio adicional para la carpeta forense; se recomiendan 600 GB de espacio en disco.
- 2GB RAM; se recomienda 4GB RAM
- Windows Server físico o virtual. Utilice uno de los siguientes:
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Internet Information Services (IIS) 7.0 o posterior conASP.NET y componentes de compresiones de contenidos estáticos
- .NET Framework:
  - Windows Server 2008 R2: .NET Framework 4 con parche KB2468871
  - Windows Server 2012: .NET Framework 3.5 y 4.5
- Aplicaciones de bases de datos—Las aplicaciones del lado del servidor requieren una base de datos SQL que sea una base de datos local instalada en el mismo servidor que el Endpoint Security Manager o una base de datos externa instalada en otra máquina. Utilice una de las siguiente aplicaciones de bases de datos:
  - SQLite 1.0.82.0 o posterior para la etapa de evaluación. Encuentre el archivo de configuración SQLite en la carpeta Herramientas de su paquete de instalación de endpoints, o descárguelo de Internet.
  - MS-SQL 2008
  - MS-SQL 2012
  - MS-SQL 2014

> Consulte al equipo de soporte de Palo Alto Networks si se requiere la integración con una base de datos existente.

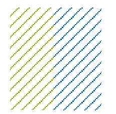
- Certificado SSL de una autoridad de certificación (CA) de confianza con autenticación del servidor y autenticación del cliente (recomendado).
- Permite la comunicación en el puerto TCP de los clientes al servidor (el puerto por defecto es 2125).
- Carpeta forense con BITS habilitado.

Consulte también: Requisitos previos para la instalación de Traps en un endpoint.

Requisitos previos para la instalación de Traps en un endpoint

Antes de instalar Traps 3.2, asegúrese de que el endpoint de destino cumple los siguientes requisitos previos:

- ESM Core y la consola ejecutando la Protección avanzada del endpoint en la misma versión que Traps o posterior.
- 200 MB de espacio en disco; se recomienda 20 GB de espacio en disco
- 512 MB RAM; se recomienda 2GB RAM
- Sistema operativo:
  - Windows XP (32-bit, SP3 o posterior)
  - Windows 7 (32-bit, 64-bit, RTM y SP1; todas las ediciones excepto Home)
  - Windows 8 (32-bit, 64-bit)
  - Windows 8.1 (32-bit, 64-bit)
  - Windows Server 2003 (32-bit, SP2 o posterior)
  - Windows Server 2003 R2 (32-bit, SP2 o posterior)
  - Windows Server 2008 (32-bit, 64-bit)
  - Windows Server 2012 (todas las ediciones)
  - Windows Server 2012 R2 (todas las ediciones)
  - Windows Vista (32-bit, 64-bit, y SP2)
- Entornos virtuales:
  - VDIs: Para consideraciones de licencias, póngase en contacto con el equipo de soporte o con su ingeniero de ventas.
  - Citrix
  - VM
  - ESX
  - VirtualBox/Parallels
- Plataformas físicas:
  - SCADA
  - Tablets Windows
- .NET 3.5 SP1
- Permita la comunicación en el puerto TCP 2125 de clientes a servidor.



Configuración de la infraestructura de Traps

Los temas siguientes muestran cómo configurar los componentes de la infraestructura de Traps:

- Configuración de la infraestructura de endpoints
- Actualización de la infraestructura de endpoints.
- Configuración del Endpoint Security Manager
- Configuración de los endpoints
- Verificar una instalación correcta

Configuración de la infraestructura de endpoints

Use el flujo de trabajo siguiente para configurar la infraestructura de endpoints o, para actualizar la infraestructura de endpoints existente, utilice el flujo de trabajo descrito en Actualización de la infraestructura de endpoints.:

Tarea		Cómo obtener más información
Paso 1	Revise los requisitos previos del software.	Consideraciones de instalación de la infraestructura de endpoints Requisitos previos para la instalación del servidor ESM Requisitos previos para la instalación de Traps en un endpoint
Paso 2	Revise las etapas de implementación recomendadas.	Etapas de implementación de Traps
Paso 3	(Opcional) Configure Internet Information Services (IIS) con .NET Services.	Habilitación de servicios web Configuración de SSL en la consola ESM
Paso 4	(Opcional) Configure el servidor MS-SQL.	Configuración de la base de datos del servidor MS-SQL
Paso 5	Instale el software del servidor ESM	Instalación del software del servidor Endpoint Security Manager
Paso 6	Instale el software de la consola ESM	Instalación del software de la consola Endpoint Security Manager
Paso 7	Instale la política de seguridad básica.	Carga de las políticas de seguridad básicas
Paso 8	Instale Traps en los endpoints.	Instalación de Traps en el endpoint Instalación de Traps en el endpoint usando Msiexec
Paso 9	Verifique si la instalación se ha realizado correctamente.	Verificar una instalación correcta

Actualización de la infraestructura de endpoints.

Utilice el siguiente flujo de trabajo para configurar la infraestructura de endpoints.

Tarea		Cómo obtener más información
Paso 1	Revise los requisitos previos del software.	Consideraciones de instalación de la infraestructura de endpoints Requisitos previos para la instalación del servidor ESM Requisitos previos para la instalación de Traps en un endpoint
Paso 2	Instale el software del servidor ESM	Instalación del software del servidor Endpoint Security Manager
Paso 3	Instale el software de la consola ESM	Instalación del software de la consola Endpoint Security Manager
Paso 4	Instale la política de seguridad básica.	Carga de las políticas de seguridad básicas
Paso 5	Instale Traps en los endpoints.	Instalación de Traps en el endpoint
Paso 6	Verifique si la instalación se ha realizado correctamente.	Verificar una instalación correcta

Configuración del Endpoint Security Manager

Consideraciones de instalación de la infraestructura de endpoints

Para instalar o actualizar los componentes del ESM, considere lo siguiente:

- El servidor ESM y la consola ESM deben tener la misma versión.
- El servidor ESM y la consola ESM son compatibles con versiones mixtas de Traps y son compatibles con versiones anteriores. Por ejemplo, un servidor ESM y consola ESM que se ejecutan con la versión 3.2 pueden aceptar endpoints que funcionan con una mezcla de agentes de Traps 3.1 y 3.2.

Para los requisitos previos de instalación, consulteRequisitos previos para la instalación del servidor ESM y Requisitos previos para la instalación de Traps en un endpoint.

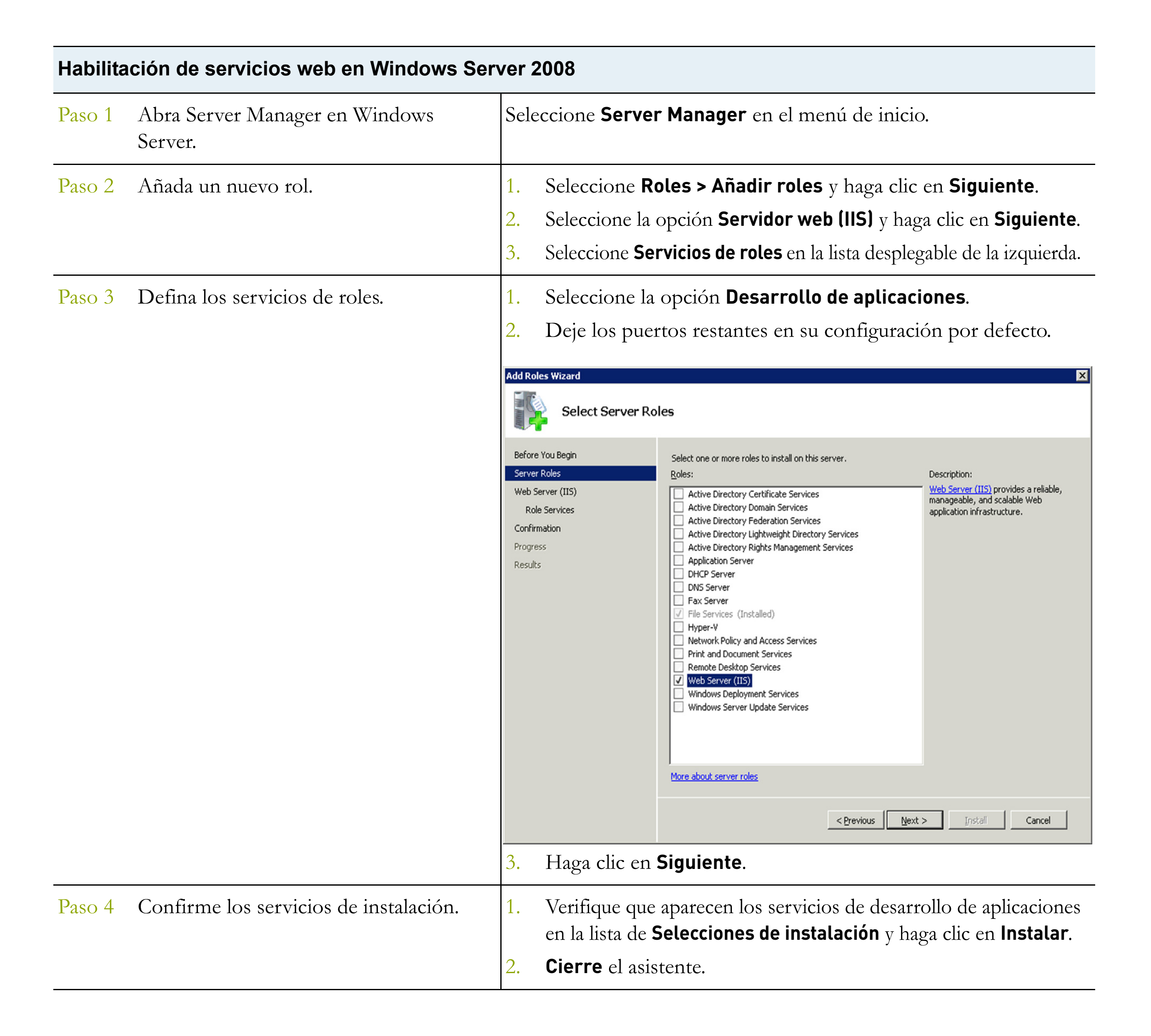
Habilitación de servicios web

Para ejecutar servicios web en el ESM, debe habilitar el papel de Internet Information Services (IIS) y .NET en un Windows Server. IIS le permite compartir información con usuarios en Internet, una intranet o una extranet. Windows Servers con IIS 7.5 proporciona una plataforma web unificada que integra IIS, ASP.NET y Windows Communication Foundation (WCF). Para acceder al Endpoint Security Manager a través de la web, habilite IIS con .NET.

Habilitación de servicios web en Windows Server 2008 R2

Para habilitar los servicios web en Windows Server 2008 R2, debe instalar .NET Framework 4 con el parche KB2468871.

Habilitación de servicios web en Windows Server 2008		
Paso 1	Abra Server Manager en Windows Server.	Seleccione **Server Manager** en el menú de inicio.
Paso 2	Añada un nuevo rol.	1. Seleccione **Roles > Añadir roles** y haga clic en **Siguiente**. 2. Seleccione la opción **Servidor web (IIS)** y haga clic en **Siguiente**. 3. Seleccione **Servicios de roles** en la lista desplegable de la izquierda.
Paso 3	Defina los servicios de roles.	1. Seleccione la opción **Desarrollo de aplicaciones**. 2. Deje los puertos restantes en su configuración por defecto.



		3. Haga clic en **Siguiente**.
Paso 4	Confirme los servicios de instalación.	1. Verifique que aparecen los servicios de desarrollo de aplicaciones en la lista de **Selecciones de instalación** y haga clic en **Instalar**. 2. **Cierre** el asistente.

Habilitación de servicios web en Windows Server 2012

Para habilitar los servicios web en Windows Server 2012, debe instalar .NET Framework 3.5 y 4.5.

Habilitación de servicios web en Windows Server 2012		
Paso 1	Abra Server Manager en Windows Server.	1. Seleccione **Server Manager** en el menú **Inicio**. 2. Seleccione **Añadir roles y características**y haga clic en **Siguiente**.
Paso 2	Seleccione el tipo de instalación.	Seleccione **Instalación basada en roles o basada en características** y haga clic en **Siguiente**.
Paso 3	Especifique el servidor.	Seleccione el servidor del grupo de servidores y haga clic en **Siguiente**.

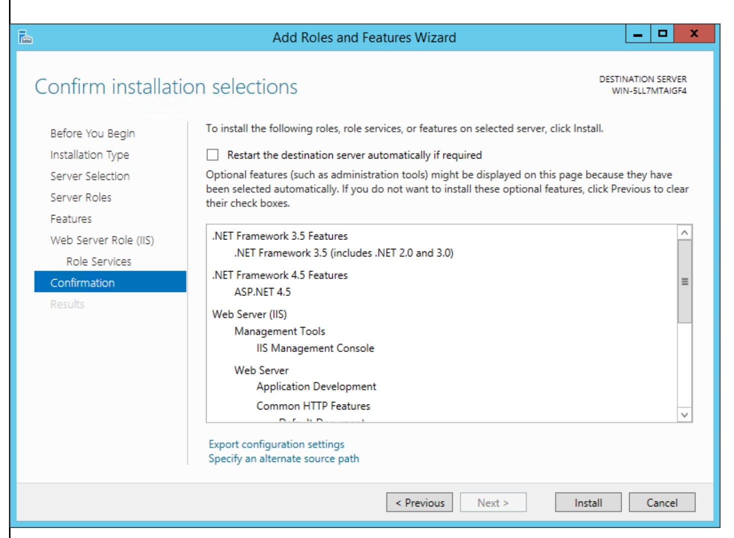
Habilitación de servicios web en Windows Server 2012 (Continuación)

Paso 4 Añada el rol y las características de Web Services.

1. Seleccione la opción **Servidor web (IIS)**.
2. Haga clic en **Añadir características**.
3. Haga clic en **Siguiente**.
4. Seleccione **Características de .NET Framework 3.5**.
5. Seleccione **Características de .NET Framework 4.5** y **ASP.NET 4.5**.
6. Haga clic en **Siguiente**. Haga clic en **Siguiente** de nuevo.
7. Bajo **Servidor web**, seleccione **Desarrollo de aplicaciones** y expanda las características para mostrar selecciones adicionales. Seleccione las características siguientes. Si así se pide, haga clic en **Añadir características**.
   - ASP.NET 3.5
   - ASP.NET 4.5
   - Extensiones de ISAPI
   - Filtros de ISAPI
   - .NET Extensibility 3.5
   - .NET Extensibility 4.5
8. Haga clic en **Siguiente**.

Paso 5 Confirme los servicios de instalación.

1. Verifique que aparecen las características en la lista de **Selecciones de instalación** y haga clic en **Instalar**.



2. Haga clic en **Cerrar** para salir del asistente.

Configuración de SSL en la consola ESM

Para la seguridad de su consola ESM y proteger la privacidad del usuario que utiliza Secure Sockets Layer (SSL), instale un certificado de servidor y añada un enlace HTTPS en el puerto 443.

Configuración de SSL en la consola ESM		
Paso 1	Abra el administrador de IIS.	1. Haga clic en **Inicio** y, a continuación en **Panel de control**. 2. Proceda con una de las siguientes opciones: • Haga clic en **Sistema y seguridad > Herramientas administrativas**. • En **Iniciar búsqueda**, escriba **inetmgr** y pulse **INTRO**.
Paso 2	(Opcional) Si su sitio requiere SSL, instale un certificado de SSL en el servidor que ejecuta la consola ESM. El certificado del servidor permite a los usuarios confirmar la identidad de un servidor web antes de transmitir datos sensibles, y utiliza la información de clave pública del servidor para encriptar datos y devolverlos al servidor. Omita este paso si su sitio no requiere SSL o si ha instalado previamente el certificado SSL.	Para solicitar o instalar un certificado de servidor, consulte: • Solicitar un certificado de servidor de Internet • Instalar un certificado de servidor de Internet
Paso 3	Añada un enlace HTTPS.	1. Bajo **Conexiones**, expanda el nodo **Sitios** del árbol y haga clic para seleccionar el sitio para el que desea un enlace. 2. Bajo **Acciones > Editar sitio**, haga clic en **Enlaces > Añadir**. 3. Especifique el tipo como https y añada la información restante del enlace, incluidos **Dirección IP**, **Puerto** (por defecto, 443), y **Nombre de host**. 4. (Opcional solo para Windows Server 2012) Seleccione la opción para **Requerir indicación de nombre de servidor**. 5. Seleccione el certificado SSL de la lista desplegable y haga clic en **ACEPTAR**.

Configuración de la base de datos del servidor MS-SQL

El Endpoint Security Manager requiere una base de datos que se gestiona a través de la plataforma MS-SQL, ya sea MS SQL 2008 o MS SQL 2012. El Endpoint Security Manager utiliza la base de datos para almacenar información administrativa, reglas de políticas de seguridad, información acerca de eventos de seguridad e información de otros tipos que utiliza el Endpoint Security Manager.



Durante la etapa de prueba de concepto, también es compatible la base de datos SQLite.

Antes de instalar el Endpoint Security Manager, debe configurar la base de datos MS-SQL con los permisos necesarios. Cuando utilice Windows Authentication como método de autenticación de usuarios, el propietario debe tener derechos de *Iniciar sesión como servicio.*

Se recomienda el procedimiento siguiente como la práctica correcta para crear y configurar una base de datos del servidor MS-SQL.

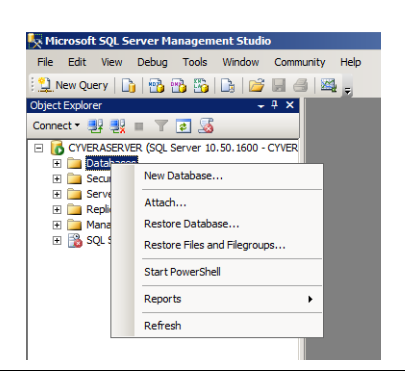
Configuración de la base de datos del servidor MS-SQL

Paso 1 Cree una nueva base de datos.

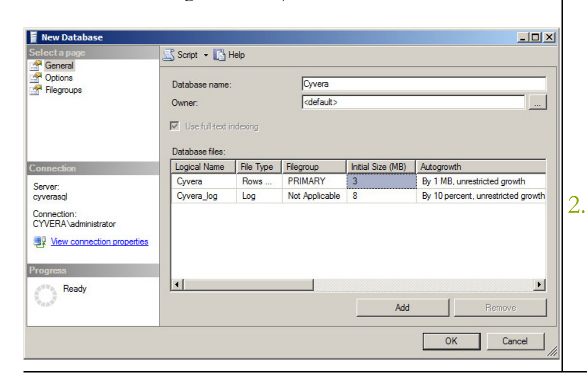
1. Seleccione **SQL Server Management Studio** en el menú Inicio.
2. Haga clic en **Conectar** para abrir Microsoft SQL Server Management Studio.



3. Seleccione **Base de datos > Nueva base de datos**....



Paso 2 Configure los ajustes de la base de datos.

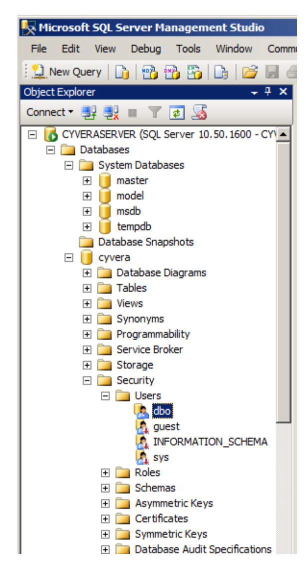


1. Introduzca la siguiente información:
   - **Nombre de la base de datos**
   - **Propietario** (incluido el dominio)



Cuando utilice Windows Authentication como método de autenticación de usuarios, el propietario debe tener derechos de "Iniciar sesión como servicio".

2. Haga clic en **ACEPTAR**.

Configuración de la base de datos del servidor MS-SQL (Continuación)	
Paso 3 Verifique el propietario de la base de datos.	1. Introduzca la información de inicio de sesión y haga clic en **Comprobar nombres**. 2. Seleccione el nombre correspondiente y haga clic en **ACEPTAR** para volver a la página Seleccionar propietario de base de datos y, de nuevo, para volver a la página de Microsoft SQL Server Management Studio. 3. Seleccione la base de datos que ha creado y, a continuación, seleccione **Seguridad > Usuarios > dbo**.  4. Verifique que se selecciona **db_owner** en las secciones Esquemas en propiedad y Miembros de roles del cuadro de diálogo Usuario de base de datos y haga clic en **ACEPTAR**.

Instalación del software del servidor Endpoint Security Manager

Antes de instalar el software del servidor del Endpoint Security Manager (ESM), verifique que el sistema cumple los requisitos que se describen en Requisitos previos para la instalación del servidor ESM.

Instalación del software del servidor del Endpoint Security Manager	
Paso 1 Inicie la instalación del software del servidor ESM	1. Obtenga el software de su administrador de cuentas de Palo Alto Networks, su vendedor o en https://support.paloaltonetworks.com. 2. Descomprima el archivo y haga doble clic en el archivo de instalación **ESMCore**. 3. En el diálogo del Contrato de licencia de usuario final, seleccione la casilla **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**. 4. Deje la carpeta de instalación por defecto, o haga clic en **Cambiar** para especificar una carpeta de instalación diferente, y haga clic en **Siguiente**.

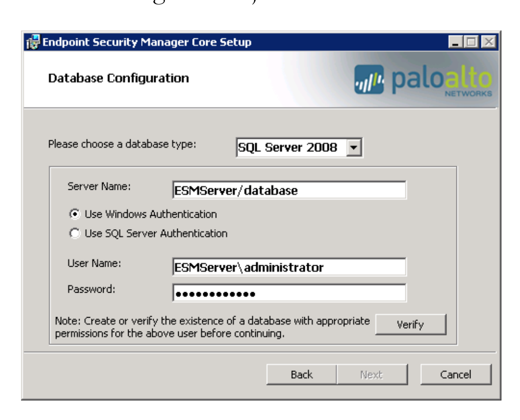
Instalación del software del servidor del Endpoint Security Manager (Continuación)

Paso 2 Configure los ajustes para el usuario administrativo.



1. Elija el tipo de autenticación que desea usar.
   - **Máquina**—El Endpoint Security Manager autentica usando los usuarios y grupos de la máquina local.
   - **Dominio**—El Endpoint Security Manager autentica los usuarios y grupos que pertenecen al dominio de la máquina.
2. Introduzca el nombre de la cuenta para el usuario que administrará el servidor en el campo **Especifique un usuario administrativo** y haga clic en **Siguiente**.

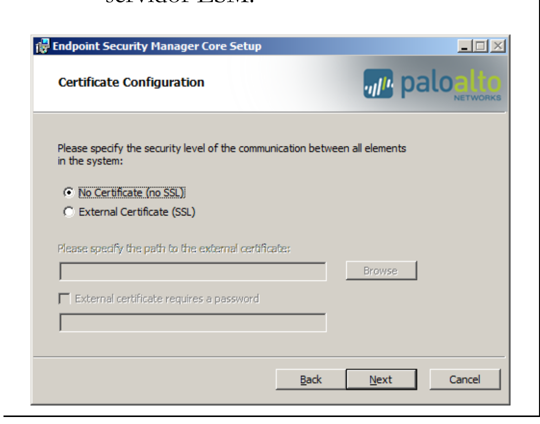
Paso 3 Configure los ajustes de la base de datos.



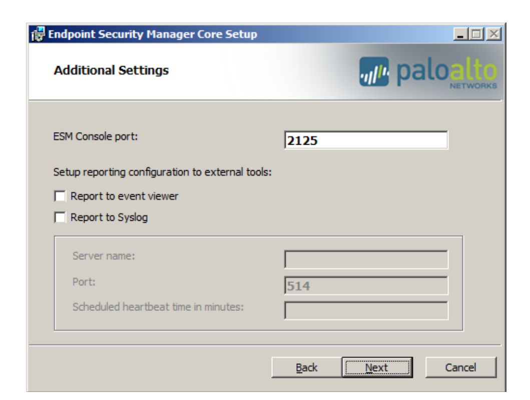
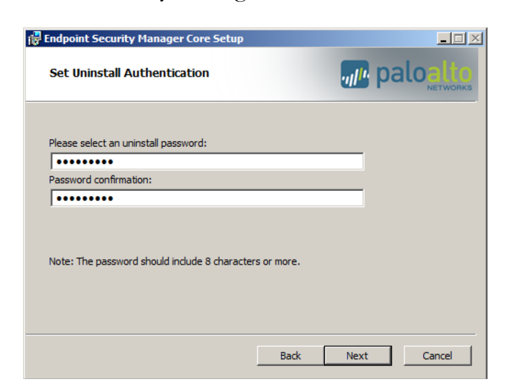
1. Seleccione el tipo de base de datos que ha instalado para su uso con Endpoint Security Manager.

   Si selecciona un servidor SQL, debe facilitar la siguiente información de configuración:
   - SQL **Nombre del servidor** o dirección IP e instancia de la base de datos (por ejemplo, ESMServer/database).
   - Tipo de autenticación (Windows o SQL).
   - Nombre de usuario, incluido el dominio (por ejemplo, ESMServer/administrator), y la contraseña para el servidor para el usuario que administrará la base de datos. La cuenta de usuario que especifique debe tener permisos para crear una base de datos en el servidor.
2. Haga clic en **Verificar** para confirmar que el servidor se puede conectar a la base de datos utilizando credenciales de autenticación. Si lo hace con éxito, haga clic en **Siguiente**.

Paso 4 Especifique el nivel de seguridad para la comunicación entre los componentes del servidor ESM.

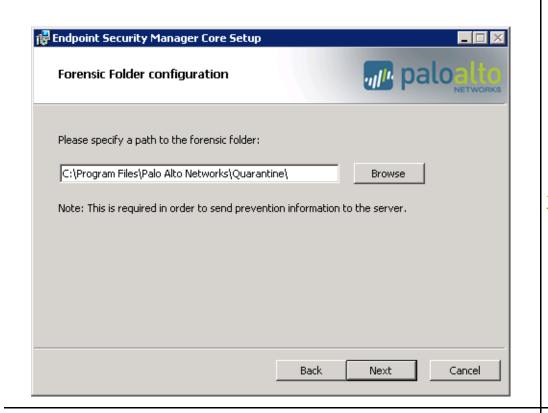


1. Seleccione una de las siguientes opciones:
   - **Sin certificado (sin SSL)**—La comunicación no se encripta (no recomendado).
   - **Certificado externo (SSL)**—Todas las comunicaciones se encriptan en SSL. Si selecciona esta opción, vaya al archivo de certificado (en formato PFX) e introduzca la contraseña necesaria para desencriptar la clave privada del archivo PFX.
2. Haga clic en **Siguiente**.

Instalación del software del servidor del Endpoint Security Manager (Continuación)	
Paso 5 Configure ajustes adicionales para su servidor ESM.  	1. Configure los siguientes ajustes, según sea necesario para su entorno: • **Puerto de consola ESM**—Especifique el puerto que va a utilizar para acceder a la interfaz web o dejar el ajuste por defecto (2125). • (Opcional) Seleccione una o más opciones de herramientas de información externas: – **Informar a visor de eventos**—Informa de todos los eventos al visor de eventos de Windows. – **Informar a Syslog**—Informa de todos los eventos a un servidor syslog externo. Introduzca el **Nombre del servidor** syslog, el **Puerto** de comunicación y la frecuencia **heartbeat programada** en minutos.  Introduzca un valor de 0 si no desea enviar información heartbeat al servidor syslog. 2. Haga clic en **Siguiente**.
Paso 6 Defina una contraseña necesaria para la desinstalación del software del Endpoint Security Manager.  	1. Introduzca y confirme una contraseña con una longitud mínima de ocho caracteres. 2. Haga clic en **Siguiente**.
Paso 7 Finalice la instalación.	1. Haga clic en **Instalar**. 2. Cuando finalice la instalación, haga clic en **Finalizar**.

Instalación del software de la consola Endpoint Security Manager

Antes de instalar el software de la consola del Endpoint Security Manager (ESM), verifique que el sistema cumple los requisitos que se describen en Requisitos previos para la instalación del servidor ESM.

Instalación del software de la consola Endpoint Security Manager		
Paso 1	Inicie la instalación del software de la consola ESM	1. Obtenga el software de su administrador de cuentas de Palo Alto Networks, su vendedor o en https://support.paloaltonetworks.com. 2. Descomprima el archivo y haga doble clic en el archivo de instalación **ESMConsole**. 3. Haga clic en **Siguiente** para comenzar el proceso de configuración. 4. Seleccione la casilla **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**.
Paso 2	Indique la carpeta de instalación para el Endpoint Security Manager.	Deje la carpeta de instalación por defecto, o haga clic en **Cambiar** para especificar una carpeta de instalación diferente, y haga clic en **Siguiente**.
Paso 3	Introduzca los ajustes de configuración de la base de datos.	1. Seleccione el tipo de base de datos que ha instalado para su uso con el ESM. Para una base de datos SQL configure: • **Nombre del servidor** SQL o dirección IP seguida por la instancia de base de datos (por ejemplo, ESMServer\database). • Tipo de autenticación (Windows o SQL). • **Nombre de usuario** incluido el dominio (por ejemplo, ESMServer/administrator) y la **Contraseña** para el servidor para el usuario que administrará la base de datos. La cuenta de usuario que especifique debe tener permisos para crear una base de datos en el servidor. 2. Haga clic en **Verificar** para confirmar que el servidor se puede conectar a la base de datos utilizando credenciales de autenticación. Si lo hace con éxito, haga clic en **Siguiente**.
Paso 4	Indique la carpeta forense. 	1. Introduzca la ruta de la carpeta forense (por defecto C:\Program Files\Palo Alto Networks\Quarantine\) o **Vaya** a la localización de la carpeta.  El instalador habilita automáticamente BITS para esta carpeta. 2. Haga clic en **Siguiente**.
Paso 5	Finalice la instalación.	1. Haga clic en **Instalar**. 2. Cuando finalice la instalación, haga clic en **Finalizar**.

Instalación del software de la consola Endpoint Security Manager (Continuación)		
Paso 6	Instale la licencia.  Debe instalar la clave de licencia antes que transcurran cinco minutos tras la instalación del software del Endpoint Security Manager. Si espera para instalar la clave de licencia, deberá reiniciar el servicio del Administrador de seguridad de endpoints.	1. Haga doble clic en el icono de la consola Endpoint Security Manager desde el escritorio o vaya a la consola (http://localhost/EndpointSecurityManager/). 2. Introduzca su identificativo y contraseña. 3. Cuando se le pida, haga clic en el enlace para **Navegar** al archivo de la clave de licencia, y haga clic en **Cargar**. 4. Inicie sesión del nuevo para acceder al panel del Endpoint Security Manager.
Paso 7	Verifique que el servicio ESM Core está activo.	1. Abra el administrador de servicios: • Windows Server 2008: En el menú de inicio, seleccione **Panel de control > Herramientas administrativas > Servicios**. • Windows Server 2012: En el menú de inicio seleccione **Panel de control > Sistema y seguridad > Herramientas administrativas > Servicios**. 2. Si el servicio ESM Core está detenido o deshabilitado, haga doble clic en el servicio y haga clic en **Inicio**.

Carga de las políticas de seguridad básicas

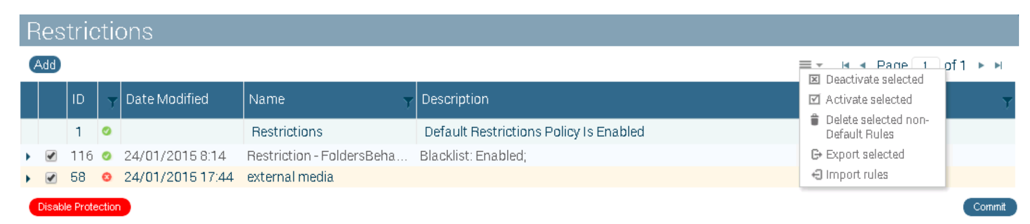
Por defecto, la política de seguridad de endpoints contiene un conjunto de reglas predefinidas que protegen los procesos comunes que se ejecutan en los endpoints. Tras instalar el software del EMS y cargar con éxito la licencia, se recomienda encarecidamente importar los archivos de seguridad básicos facilitados por Palo Alto Networks. Las políticas solucionan problemas de compatibilidad, así como problemas de estabilidad con prevención de malware y módulos de inyección de subprocesos, y configuran notificaciones acerca de los ejecutables que se ejecutan de medios externos y carpetas del sistema operativo.

Puede importar las políticas de seguridad básicas de cualquier página de reglas, donde se pueden importar (restricciones, EPM, etc.).

Importación de las políticas de seguridad básicas	
Paso 1	Descargue las políticas de https://live.paloaltonetworks.com/docs/DOC-7829 u guárdelas en una carpeta local o una carpeta de red a la que pueda acceder desde el Endpoint Security Manager.
Paso 2	En el Endpoint Security Manager, abra una página de administración de reglas, por ejemplo, **Políticas > Malware > Restricciones**.

Importación de las políticas de seguridad básicas (Continuación)

Paso 3 Seleccione **Importar reglas** en el menú ≡ ▾. **Vaya** al archivo de políticas, y haga clic en **Cargar**.



El Endpoint Security Manager añade la nueva regla o reglas a la política de seguridad existente y asigna un número de ID único a cada regla. Repita el Step 3 para cada política. La consola ESM muestra las reglas en una página de administración dedicada para cada tipo de regla.

Para más información acerca de la importación o exportaciones de reglas de políticas, consulte Exportación e importación de archivos de las políticas.

Configuración de los endpoints

Para configurar Traps en los endpoints de su organización, consulte los temas siguientes:

▲ Etapas de implementación de Traps
▲ Consideraciones de instalación de Traps
▲ Instalación de Traps en el endpoint
▲ Instalación de Traps en el endpoint usando Msiexec

Etapas de implementación de Traps

El software Traps suele implementarse en los endpoints de una red tras una prueba de concepto (POC) inicial, que simula el entorno de producción de la empresa. Durante la etapa de POC o de implementación, se analizan los eventos de seguridad para determinar cuáles de ellos se deben a actividades malintencionadas, y los que se deben a procesos legítimos que se comparten de una manera incorrecta o con riesgo. También puede simular el número y tipos de endpoints de la organización, los perfiles de usuario y los tipos de aplicaciones que se ejecutan en los endpoints. De acuerdo a estos factores, se define, se prueba y se ajusta la política de seguridad acorde a su organización.

El objetivo del proceso de pasos múltiples es proporcionar la máxima protección a su organización, al tiempo que no interfiere en los flujos de trabajo legítimos.

Tras la POC inicial, se recomienda una implementación de pasos múltiples por las razones siguientes:

- La POC no siempre refleja todos los entornos de producción.
- Existe una escasa probabilidad de que el software Traps afecte a las aplicaciones específicas, lo que puede revelar vulnerabilidades en el software como un ataque prevenido.
- El aislamiento de los problemas que aparecen y su solución son más sencillos cuando no afecta a un entorno grande o a un número de usuarios potencialmente grande.

La implementación de pasos múltiples garantiza una implementación adecuada del software de Traps en toda la red. Estos pasos permiten un mejor soporte y control sobre la protección añadida.

Paso		Duración	Plan
Paso 1	Instale Traps en los endpoints.	1 semana	Instale el Endpoint Security Manager (ESM) incluida una base de datos MS SQL, la consola ESM y el servidor ESM, e instale Traps en algunos (3-10) endpoints. Compruebe el funcionamiento normal de los agentes de Traps (inyección, política) y verifique que no hay cambios en la experiencia del usuario.
Paso 2	Expanda la implementación de Traps.	2 semanas	Expanda gradualmente la distribución de agentes a grupos más grandes con atributos similares (hardware, software, usuarios). Transcurridas dos semanas, puede tener hasta 100 endpoints instalados.
Paso 3	Finalice la instalación de Traps.	2 o más semanas	Haga una distribución amplia de los clientes en la organización.

Paso		Duración	Plan
Paso 4	Defina la política de la empresa y los procesos protegidos.	Hasta una semana	Añada reglas de protección para aplicaciones de terceros o propias y compruébelas con el probador de compatibilidad de endpoints.
Paso 5	Refine la política de la empresa y los procesos protegidos.	Hasta una semana	Implemente reglas de protección en un pequeño número de endpoints que utilicen las aplicaciones con frecuencia. Ajuste la política según sea necesario.
Paso 6	Finalice la política de la empresa y los procesos protegidos.	Unos minutos.	Implemente las reglas globalmente.

Consideraciones de instalación de Traps

Puede instalar Traps de las formas siguientes:

- En situaciones en las que necesita instalar Traps en un pequeño número de endpoints, puede instalar el software Traps manualmente utilizando el flujo de trabajo descrito en Instalación de Traps en el endpoint.
- Para instalar Traps desde la línea de comandos, use la utilidad Msiexec para realizar operaciones en un instalador de Windows, como se describe en Instalación de Traps en el endpoint usando Msiexec. También puede utilizar las opciones de instalación de Msiexec con software de implementación de MSI, como Policy System Center Configuration Manager (SCCM), Altiris, o Group Policy Object (GPO). Se recomienda utilizar software de implementación de MSI para instalar Traps en toda una organización o un número elevado de endpoints.
- Si los endpoints de su organización ya tienen instalado Traps, puede actualizar el software Traps configurando una regla de acción, según se describe en Desinstalación o actualización de Traps en el endpoint.

Instalación de Traps en el endpoint

Antes de instalar Traps, verifique que el sistema cumple los requisitos que se describen en Requisitos previos para la instalación de Traps en un endpoint.

Instalación de Traps en el endpoint		
Paso 1	Inicie la instalación del software Traps.  Las versión o versiones de Traps que instale en sus endpoints debe ser la misma o anterior a la versión de ESM Core y la consola.	1. Obtenga el software de su administrador de cuentas de Palo Alto Networks, su vendedor o en https://support.paloaltonetworks.com. 2. Descomprima el archivo y haga doble clic en el archivo de instalación **Traps**, x64 o x68. 3. Haga clic en **Siguiente**. 4. Seleccione la casilla **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**.

Instalación de Traps en el endpoint		
Paso 2	Configure los agentes de Traps para conectarlos al servidor ESM.	Puede configurar el agente de Traps para su conexión a un servidor principal o secundario. Si no puede acceder al servidor principal, el agente de Traps intenta ponerse en contacto con el servidor secundario. 1. Proporcione la siguiente información para el servidor ESM: • **Nombre del host**—Introduzca el nombre del host o la dirección IP del servidor ESM. • **Puerto**—Si es necesario, cambie el número de puerto (por defecto es 2125). • **Uso**—Seleccione **SSL** para encriptar la comunicación con el servidor o **No SSL** para no encriptarla. 2. Haga clic en **Siguiente** en los mensajes que aparezcan para finalizar la instalación.  Se recomienda reiniciar el ordenador tras finalizar la instalación.

Instalación de Traps en el endpoint usando Msiexec

Windows Msiexec le proporciona un control completo del proceso de instalación y le permite instalar, modificar y realizar operaciones en un instalador de Windows desde la línea de comandos. Cuando se utiliza junto con un System Center Configuration Manager (SCCM), Altiris, Group Policy Object (GPO), o u otras aplicaciones de implementación de MSI, Msiexec le permite instalar Traps en múltiples endpoints de su organización (por primera vez). Tras instalar con éxito Traps en un endpoint y establecer una conexión con el Endpoint Security Manager, puede configurar reglas para actualizar o desinstalar Traps (consulte Desinstalación o actualización de Traps en el endpoint).

Antes de instalar Traps, verifique que el sistema cumple los requisitos que se describen en Requisitos previos para la instalación de Traps en un endpoint.

Instalación de Traps en el endpoint usando Msiexec	
Paso 1	Abra una línea de comando como administrador: • Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**. • Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL+Mayús.+INTRO**.

Instalación de Traps en el endpoint usando Msiexec (Continuación)

Paso 2 Ejecute el comando `Msiexec` seguido de una o más de las siguientes opciones o propiedades:

- Opciones de instalación, visualización y logging:
  - `/i <installpath>\<installerfilename>.msi`—Instalar un paquete. Por ejemplo, `msiexec /i c:\install\traps.msi`.
  - `/qn`—No muestra ninguna interfaz de usuario (instalación silenciosa). Como mínimo, debe especificar el nombre del servidor host o la dirección IP usando la propiedad `CYVERA_SERVER`.
  - `/L*v <logpath>/<logfilename>.txt`—Salida verbose de log a un archivo. Por ejemplo, `/L*v c:\logs\install.txt`.
  - `/x <installpath>\<installerfilename>.msi>.txt`—Desintalar un paquete. Por ejemplo, `msiexec /x c:\install\traps.msi`.

  Para una lista completa de los parámetros de Msiexec, consulte https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/msiexec.mspx
- Propiedades públicas:
  - `CYVERA_SERVER="<servername>"`—Nombre de servidor host principal o dirección IP (por defecto es CyveraServer)
  - `CYVERA_SERVER_PORT="<serverport>"`—Puerto de servidor host principal (por defecto es 2125)
  - `SSL_TYPE="[No SSL|SSL]"`—(Solo instalación no silenciosa) Define las preferencias de encriptación del servidor principal especificando No SSL (por defecto) o SSL
  - `USE_SSL_PRIMARY="[0|1]"`—(Solo instalación silenciosa) Define las preferencias de encriptación del servidor principal especificando un 0 para no usar SSL o un 1 para usar SSL (por defecto)
  - `USE_BACKUP_SERVER="[0|1]"`—Define las preferencias de copia de respaldo especificando 0 (por defecto) para no utilizar un servidor de copia de respaldo o 1 para utilizar un servidor de copia de respaldo
  - `CYVERA_SERVER="<servername>"`—Nombre de servidor host principal o dirección IP (por defecto es CyveraServer)
  - `CYVERA_BACKUP_SERVER_PORT="<serverport>"`—Puerto de servidor host secundario (por defecto es 2125)
  - `SSL_TYPE_BACKUP="[No SSL|SSL]"`—(Solo instalación no silenciosa) Define las preferencias de encriptación del servidor secundario especificando No SSL (por defecto) o SSL
  - `USE_SSL_BACKUP="[0|1]"`——(Solo instalación silenciosa) Define las preferencias de encriptación del servidor secundario especificando un 0 para no usar SSL o un 1 para usar SSL (por defecto)
  - `UNINSTALL_PASSWORD="<uninstallpassword>"`—Introduzca la contraseña de administrador.

Por ejemplo, para instalar Traps sin una interfaz de usuario y para especificar un servidor principal con el nombre ESMServer, un servidor de respaldo con el nombre ESMServerBackup, y encriptación SSL para ambos servidores, introduzca lo siguiente:

```
msiexec /i c:\install\traps.msi /qn CYVERA_SERVER="ESMServer" USE_SSL_PRIMARY="1"
USE_BACKUP_SERVER="1" CYVERA_BACKUP_SERVER="ESMServer-Backup" USE_SSL_BACKUP="1"
```



Se recomienda reiniciar el ordenador tras finalizar la instalación.

Para desinstalar Traps y una salida verbose del log a un archivo llamado uninstallLogFile.txt, introduzca lo siguiente:

```
msiexec /x c:\install\traps.msi UNINSTALL_PASSWORD=[palo@lt0] /l*v
c:\install\uninstallLogFile.txt
```



Debe especificar la propiedad `UNINSTALL_PASSWORD` para desinstalar el paquete con éxito.

Verificar una instalación correcta

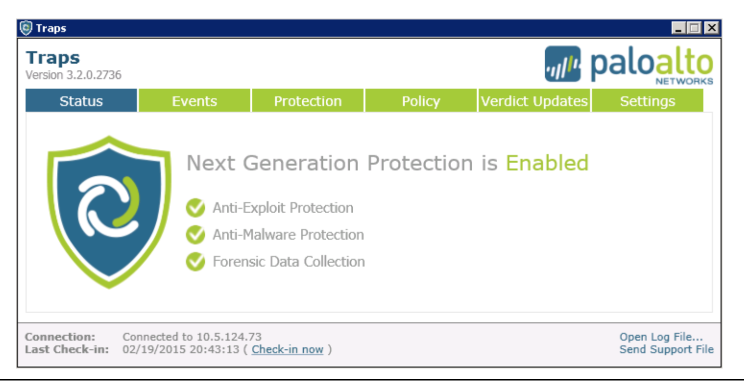
Puede verificar si una instalación se ha realizado con éxito en el servidor y el endpoint comprobando la conectividad entre el servidor y el endpoint en ambos lados de la conexión.

▲ Verificar la conectividad desde el endpoint

▲ Verificar la conectividad desde la consola ESM

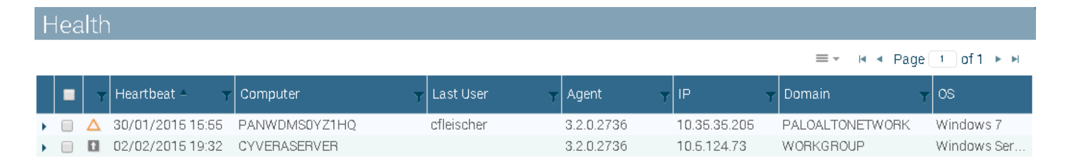
Verificar la conectividad desde el endpoint

Tras instalar con éxito Traps, el agente de Traps deberá poder conectarse con el servidor que ejecuta el Endpoint Security Manager.

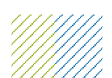
Verificar la conectividad desde el endpoint	
Paso 1	Inicie la consola de Traps desde la barra de herramientas: • En la bandeja de Windows, haga clic con el botón derecho en el icono de Traps y seleccione la **Consola**, o haga doble clic en el icono. • Ejecute CyveraConsole.exe desde la pantalla de instalación de Traps.
Paso 2	Compruebe el estado de la conexión del servidor. Si Traps está conectado al servidor, el estado **Conexión** indica que la conexión se ha realizado con éxito. Si el agente de Traps no puede establecer una conexión con el servidor principal o secundario, la consola de Traps indica el estado desconectado. 
Paso 3	Verificar la conectividad desde la consola ESM.

Verificar la conectividad desde la consola ESM

Tras verificar con éxito que el endpoint puede llegar al servidor del Endpoint Security Manager (ESM), verifique que el endpoint aparece en la lista de equipos en la página **Monitorizado > Estado** de la consola ESM.



Verificar la conectividad desde la consola ESM	
Paso 1	En la consola ESM, seleccione **Monitorizar > Estado**.
Paso 2	Verifique el estado del endpoint, localice el nombre del endpoint en la lista de equipos. Un icono indica que se está ejecutando Traps en el endpoint. Para ver detalles adicionales acerca del endpoint, seleccione la fila de endpoints.



Administración del servidor ESM

- Gestión de múltiples servidores ESM
- Gestión de las licencias del Endpoint Security Manager
- Configuración del acceso administrativo
- Exportación e importación de archivos de las políticas

Gestión de múltiples servidores ESM

Para admitir implementaciones a gran escala de múltiples sitios, puede configurar y gestionar múltiples servidores Endpoint Security Manager (ESMs) desde la consola ESM. Cada uno de los servidores ESM se conecta a una base de datos compartida donde se almacenan políticas de seguridad e información relacionada con los agentes y eventos de Traps, con capacidad para hasta 50.000 agentes de Traps, y permite la carga de datos forenses en una carga forense dedicada. Añadir servidores ESM adicionales le permite escalar el número de conexiones de Traps.

En intervalos regulares, cada servidor ESM solicita a la base de datos una lista de servidores conocidos y envía esa lista a los agentes de Traps rápidamente. Antes de iniciar una conexión, Traps determina cuál de los servidores puede conectarse con mayor rapidez e intenta establecer una conexión. Si Traps no puede establecer una conexión, baja en la lista hasta poder establecer una conexión con el servidor ESM. Si se elimina o se deshabilita temporalmente un servidor ESM, la consola ESM actualiza la lista de servidores ESM disponibles y la envía a los agentes de Traps rápidamente.

En situaciones que requieren un equilibrador de carga para gestionar el tráfico entre múltiples servidores ESM, se puede añadir la dirección IP y el nombre del host del equilibrador de carga en el lugar del servidor o servidores ESM en la consola ESM. De ese modo, el servidor ESM envía la dirección IP del equilibrador de carga como un “servidor” disponible. Los agentes de Traps pueden entonces establecer conexiones a través del equilibrador de carga, en vez de una conexión directa con el servidores o servidores ESM.

También se puede definir la carpeta forense por defecto que Traps utilizará si no se puede acceder a la carpeta asociada con el servidor ESM.

▲ Requisitos del sistema
▲ Limitaciones
▲ Gestionar servidores ESM

Requisitos del sistema

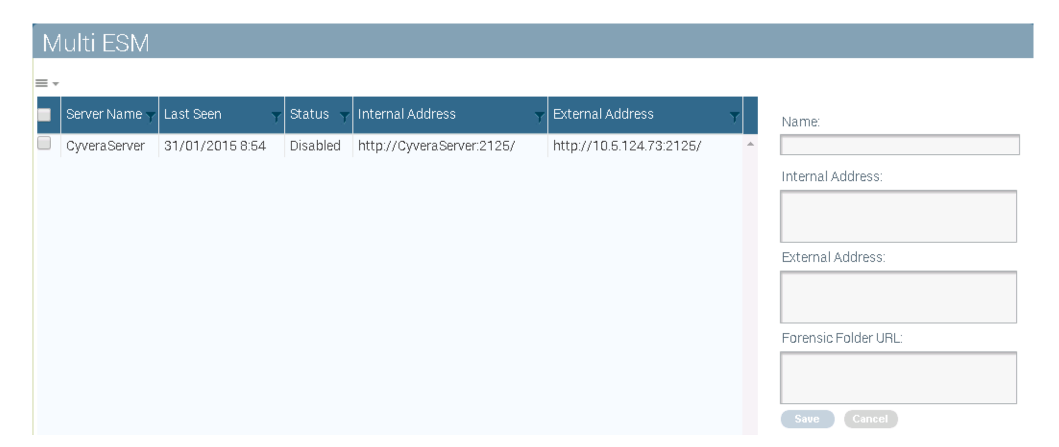
Todos los servidores ESM deben cummplir los requisitos especificados en Requisitos previos para la instalación del servidor ESM.

Limitaciones

Las implementaciones de múltiples ESM tienen las siguientes limitaciones:

- Para utilizar un equilibrador de carga, debe especificarse su dirección IP como la dirección IP interna para cada servidor ESM que se añade. Esto garantiza que los agentes de Traps se conecten con la dirección IP del equilibrador de carga, en vez de conectarse directamente con el servidor ESM.
- Cada servidor ESM debe tener una dirección IP estática.

Gestionar servidores ESM



Tras instalar los servidores ESM (véase Instalación del software del servidor Endpoint Security Manager), la consola ESM muestra información de identificación acerca de cada servidor en la página **Configuración > ESM múltiples**. Puede modificar los ajustes de configuración para los servidores ESM en cualquier momento. También puede deshabilitar temporalmente o eliminar un servidor ESM, según sea necesario.

Gestione servidores ESM

Paso 1 Seleccione el servidor ESM y, opcionalmente, modifique cualquiera de los ajustes siguientes:

- Nombre de host del servidor
- Dirección interna y puerto del servidor (por ejemplo, http://ESMServer1:2125/)
- Dirección externa y puerto del servidor que Traps utiliza para comunicarse con el servidor (por ejemplo, http://10.5.0124.73:2125/)
- Carpeta forense (por ejemplo, http://ESMSERVER:80/BitsUploads)

 Si se utiliza SSL para la comunicación con la carpeta forense, incluya el nombre de dominio totalmente cualificado (FQDN), por ejemplo **HTTPS://ESMserver.Domain.local:443/BitsUploads**.

 Para especificar la carpeta forense por defecto cuando no se puede acceder a la carpeta asociada con el servidor ESM, seleccione **Configuración > General > Configuración del servidor**, e introduzca la **URL de la carpeta forense**.

Paso 2 **Guarde** sus cambios.

Paso 3 (Opcional) Para eliminar o deshabilitar temporalmente un ESM, seleccione la acción del ≡ ▾ menú de la parte superior de la página. Esta acción elimina el servidor ESM del conjunto de servidores disponibles desde el que pueden conectarse los agentes de Traps.

Gestión de las licencias del Endpoint Security Manager

Antes de poder utilizar la consola Endpoint Security Manager (ESM), deber obtener y activar la licencia. La licencia impone la fecha de vencimiento y el número máximo de endpoints que usted puede gestionar. Los endpoints obtienen sus licencias del servidor ESM. Cada licencia especifica el tipo de licencias, el tamaño del conjunto de agentes y la fecha de vencimiento.

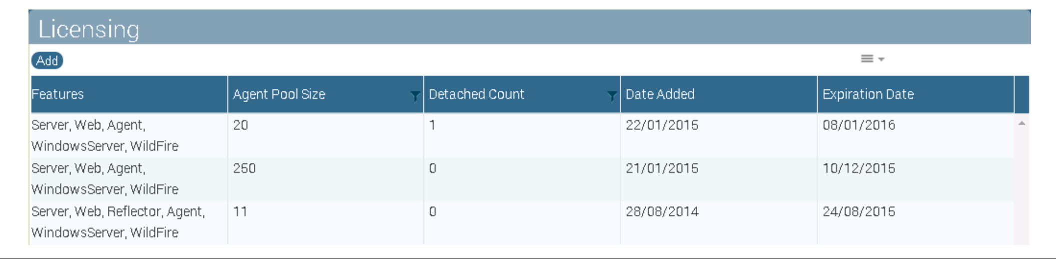
Cada instancia de base de datos requiere una licencia válida que le permite gestionar la política de seguridad del endpoint, habilitar WilFire y obtener soporte. Para adquirir licencias, póngase en contacto con su ingeniero de cuentas de Palo Alto Networks o su distribuidor.

Tras obtener una licencia, impórtela a la base de datos utilizando uno de los métodos siguientes:

- Administración de las licencias Endpoint Security Manager usando la consola ESM
- Administración de las licencias de Endpoint Security Manager usando la herramienta de configuración DB

Administración de las licencias Endpoint Security Manager usando la consola ESM

Administrar Endpoint Security Manager licencias usando la consola ESM	
Paso 1	Localice el archivo de su licencia.
Paso 2	Seleccione **Configuración > Licencias** y, a continuación **Añadir** una nueva licencia.



Features	Agent Pool Size	Detached Count	Date Added	Expiration Date
Server, Web, Agent, WindowsServer, WildFire	20	1	22/01/2015	08/01/2016
Server, Web, Agent, WindowsServer, WildFire	250	0	21/01/2015	10/12/2015
Server, Web, Reflector, Agent, WindowsServer, WildFire	11	0	28/08/2014	24/08/2015

Paso 3	**Acceda** y **Cargue** el archivo de licencia. La consola ESM muestra información acerca de la nueva licencia.
Paso 4	(Opcional) Para verificar la utilización de la licencia de Traps, seleccione **Panel** y acceda a **Capacidad de la licencia**.
Paso 5	(Opcional) Para enviar la nueva licencia a los endpoints que están cerca de la fecha de vencimiento de la licencia o la han superado, cree una regla de acción (consulte Actualización o revocación de la licencia de Traps en el endpoint).
Paso 6	(Opcional) Para exportar la información de la licencia a un archivo CSV, haga clic en el icono de menú ≡ ▾ y, a continuación, seleccione **Exportar logs**.

Administrar Endpoint Security Manager licencias usando la consola ESM	
Paso 7	Verifique que se Endpoint Security Manager está ejecutando el servicio básico en el servidor ESM: 1. Abra el administrador de servicios: • Windows Server 2008: En el menú de inicio, seleccione **Panel de contro > Herramientas administrativas > Servicios**. • Windows Server 2012: En el menú de inicio seleccione **Panel de control > Sistema y seguridad > Herramientas administrativas > Servicios**. 2. Localice el Endpoint Security Manager servicio básico (denominado CyveraServer en versiones anteriores del Endpoint Security Manager) y verifique que el estado del servicio **Iniciado** (Windows Server 2008) o **En ejecución** (Windows Server 2012). 3. Si el estado del servicio es **Detenido** o **En pausa**, haga doble clic en el servicio y seleccione **Inicio**. Haga clic en **Cerrar**.

Administración de las licencias de Endpoint Security Manager usando la herramienta de configuración DB

La herramienta de configuración DB es una interfaz de línea de comandos que proporciona una alternativa a la gestión de los ajustes básicos del servidor utilizando la consola EMS. Puede acceder a la herramienta de configuración DB utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. La herramienta de configuración DB se encuentra en la carpeta Servidor del servidor ESM.



Todos los comandos ejecutados utilizando la herramienta de configuración DB hacen distinción entre mayúsculas y minúsculas.

Administrar Endpoint Security Manager licencias usando la herramienta de configuración DB	
Paso 1	Localice el archivo de su licencia.
Paso 2	Abra una línea de comando como administrador: • Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**. • Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL**+**Mayús.**+**INTRO**.
Paso 3	Vaya a la carpeta que contiene la herramienta de configuración DB: `C:\Users\Administrator>`**`cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server`**
Paso 4	Cargue la nueva licencia: `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig importlicense C:\<PathtoLicenseFile>\<LicenseFilename>.xml`** La herramienta de configuración DB carga el archivo de licencia. Para verificar la licencia usando la consola ESM, consulte Administración de las licencias Endpoint Security Manager usando la consola ESM.
Paso 5	(Opcional) Si es necesario, cree una regla de acción en la consola ESM para enviar la nueva licencia a los endpoints (consulte Actualización o revocación de la licencia de Traps en el endpoint).

Configuración del acceso administrativo

Cuando instale la consola Endpoint Security Manager (ESM), especifique la cuenta administrativa y el tipo de autenticación que los administradores utilizarán para acceder a la consola. Tras la instalación, puede cambiar el modo de autenticación a una cuenta local o una cuenta de dominio definida en el Directorio activo, una o más cuentas administrativas, y/o cualquier grupo o grupos de autenticación que se utilicen para acceso administrativo.

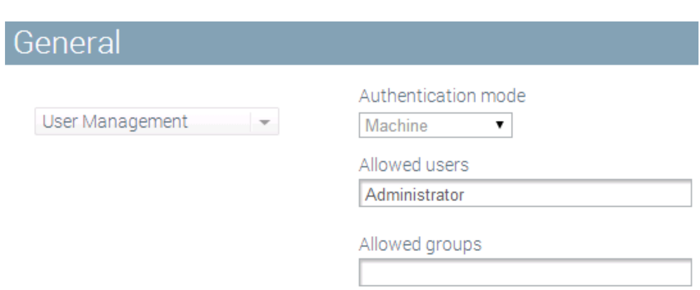
Para la configuración de ajustes avanzados, como módulos de protección contra exploits (EPM), debe introducir la contraseña de modo ninja. Puede cambiar la contraseña con la herramienta de configuración DB.

- Configuración de acceso administrativo al Endpoint Security Manager utilizando la consola ESM
- Configuración de acceso administrativo al Endpoint Security Manager utilizando la herramienta de configuración DB
- Cambio de la contraseña de modo ninja utilizando la herramienta de configuración DB

Configuración de acceso administrativo al Endpoint Security Manager utilizando la consola ESM

Cuando instale la consola Endpoint Security Manager (ESM), especifique la cuenta administrativa y el tipo de autenticación que los administradores utilizarán para acceder a la consola. Puede cambiar estas preferencias usando la herramienta de configuración de bases de datos (DB) (consulte Configuración de acceso administrativo al Endpoint Security Manager utilizando la herramienta de configuración DB) o con la consola ESM. También puede especificar el uso de un grupo de autenticación preexistente para el acceso administrativo. Por defecto, no se especifica ningún grupo.

Configuración de acceso administrativo al Endpoint Security Manager utilizando la consola ESM	
Paso 1	Seleccione **Configuración > General > Administración de usuarios**.



Paso 2	(Opcional) Seleccione el **Modo de autenticación**, ya sea **Máquina** para utilizar una cuenta local, o **Dominio** para usa una cuenta definida en el Directorio activo.
Paso 3	(Opcional) Especifique administradores adicionales en el campo **Usuarios permitidos**. Utilice un punto y coma para separar valores múltiples. Por ejemplo, <username1>;<username2>.
Paso 4	(Opcional) Especifique **Grupos permitidos**. Utilice un punto y coma para separar valores múltiples. Por ejemplo, <group1>;<group2>.

Configuración de acceso administrativo al Endpoint Security Manager utilizando la herramienta de configuración DB

Cuando instale la consola Endpoint Security Manager (ESM), especifique la cuenta administrativa y el tipo de autenticación que los administradores utilizarán para acceder al servidor. También puede especificar el uso de un grupo de autenticación preexistente para el acceso administrativo. Por defecto, no se especifica ningún grupo. Puede cambiar estas preferencias usando la consola ESM (consulte Configuración de acceso administrativo al Endpoint Security Manager utilizando la consola ESM) o usando la herramienta de configuración de bases de datos (DB).

La herramienta de configuración DB es una interfaz de línea de comandos que proporciona una alternativa a la gestión de los ajustes básicos del servidor utilizando la consola EMS. Puede acceder a la herramienta de configuración DB utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. La herramienta de configuración DB se encuentra en la carpeta Servidor del servidor ESM.



Todos los comandos ejecutados utilizando la herramienta de configuración DB hacen distinción entre mayúsculas y minúsculas.

Configuración de acceso administrativo al Endpoint Security Manager utilizando la herramienta de configuración DB	
Paso 1	Abra una línea de comando como administrador: • Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**. • Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL**+**Mayús.**+**INTRO**.
Paso 2	Vaya a la carpeta que contiene la herramienta de configuración DB: `C:\Users\Administrator>`**`cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server`**

Paso 3	(Opcional) Visualice los ajustes de administrador existentes:
	`C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig usermanagement show`**
	`AuthMode = Machine`
	`AllowedUsers = Administrator`
	`AllowedGroups =`

Paso 4	(Opcional) Especifique el modo de autenticación, dominio o máquina. `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig usermanagement authmode [domain`|`machine]`**
Paso 5	(Opcional) Especifique usuarios administrativos adicionales. Utilice un punto y coma para separar valores múltiples. Por ejemplo, administrator1;administrator2. `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig usermanagement allowedusers <username1>;<username2>`**  Los usuarios administrativos que especifique anularán cualquier valor definido previamente. Para conservar el valor o valores actuales, debe especificarlos en el comando.

Configuración de acceso administrativo al Endpoint Security Manager utilizando la herramienta de configuración DB

Paso 6 (Opcional) Especifique grupos administrativos adicionales. Utilice un punto y coma para separar valores múltiples. Por ejemplo, securityadmins;endpointadmins.

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig
usermanagement allowedgroups <groupname1>;<groupname2>
```



El grupo o grupos administrativos que especifique anularán cualquier valor definido previamente. Para conservar el valor o valores actuales, debe especificarlos en el comando.

Cambio de la contraseña de modo ninja utilizando la herramienta de configuración DB

Los módulos EMP (Advanced Exploitation Prevention Modules) están ocultos y solo se puede acceder a ellos en el modo ninja. Para visualizar los EPM avanzados, deberá introducir la contraseña de modo ninja. Para cambiar la contraseña, utilice la herramienta de configuración DB.

Cambio de la contraseña de modo ninja utilizando la herramienta de configuración DB

Paso 1 Abra una línea de comando como administrador:

- Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**.
- Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL**+**Mayús.**+**INTRO**.

Paso 2 Vaya a la carpeta que contiene la herramienta de configuración DB:

```
C:\Users\Administrator>cd C:\Program Files\Palo Alto Networks\Endpoint Security
Manager\Server
```

Paso 3 (Opcional) Visualice los ajustes de servidor existentes:

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig server show
PreventionsDestFolder = \\ESMServer\Quarantine
InventoryInterval = 284
HeartBeatGracePeriod = 300
NinjaModePassword = Password2
```

Paso 4 Especifique la nueva contraseña del modo ninja.

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig server
ninjamodepassword <password>
```

Exportación e importación de archivos de las políticas

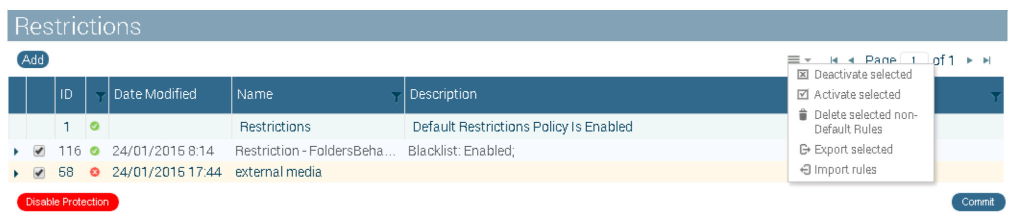
Las funciones de importación y exportación de la consola Endpoint Security Manager (ESM) le permiten hacer copias de seguridad de las reglas antes de la migración o actualización a un nuevo servidor o antes de implementar una política en múltiples servidores independientes. Puede exportar reglas de políticas de forma global o individual y guardarlas en un archivo XML. La importación de reglas de las políticas añade las reglas a la política existente y asigna un número de ID único a cada nueva regla. En Protección avanzada del endpoint 3.2, cada tipo de regla de política tiene su propia página de administración, desde la cual puede hacer una copia de seguridad o importar la reglas de las políticas de ese tipo.



Cuando se carga un archivo de políticas que contiene reglas de diferentes tipos, por ejemplo, reglas de prevención de acción y exploit, la consola ESM carga y posteriormente visualiza las políticas en sus respectivas páginas de administración.

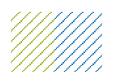
Exportación e importación de archivos de las políticas

Paso 1 Seleccione la página de administración de políticas para el conjunto de reglas que va a importar, por ejemplo, **Políticas > Malware > Restricciones**.



Paso 2 Proceda con una de las siguientes opciones:

- Para copias de seguridad o exportación de reglas de políticas, seleccione la casilla junto a las reglas que desea exportar. En el ≡ ▾ menú de la parte superior de la tabla, seleccione **Exportar seleccionados**. El Endpoint Security Manager guarda las reglas seleccionadas en un archivo XML.
- Para restaurar o importar nuevas reglas de políticas, seleccione **Importar reglas** en el ≡ ▾ menú de la parte superior de la tabla. Vaya al archivo de políticas, y haga clic en **Cargar**.



Primeros pasos con las reglas

Los temas siguientes describen los componentes básicos y los procesos asociados con cada regla:

- Descripción general de las reglas de políticas de endpoints
- Componentes y acciones comunes de las reglas

Descripción general de las reglas de políticas de endpoints

Tipos de reglas de políticas

Las políticas le permiten aplicar reglas y realizar acciones. Las diferentes reglas de políticas son altamente configurables y trabajan juntas para la administración de procesos, archivos ejecutables y ajustes en sus endpoints.

La tabla siguiente describe los tipos de reglas de políticas que se pueden configurar en la consola ESM

Tipo de regla	Descripción
Prevención de exploits	Las reglas de prevención de exploits determinan el método de protección para los procesos que se ejecutan en los endpoints. Cada regla de la política de prevención de exploits especifica el tipo de módulos de protección que protegen los procesos. Para obtener más información, consulte Reglas de protección de exploits.
Prevención de malware.	Las reglas de prevención de malware determinan el método de protección para los ejecutables que se ejecutan en los endpoints. Cada regla de la política de prevención de malware especifica el tipo de módulos de protección que protegen los ejecutables y procesos. Para obtener más información, consulte Reglas de prevención de malware.
Restricción	Las reglas de restricción determinan las restricciones o excepciones colocadas en los ejecutables que se activan en los endpoints. Para obtener más información, consulte Reglas de restricción.
WildFire	Las reglas de WildFire habilitan el análisis pre y post prevención de ejecutables enviando hashes de archivos ejecutables y opcionalmente archivos desconocidos a la nube de WildFire. Para obtener más información, consulte Reglas de WildFire.
Datos forenses	Las reglas forenses permiten definir preferencias acerca del volcado de memoria y la recopilación de archivos forenses. Para obtener más información, consulte Reglas forenses.
Ajustes de agentes	Las reglas de ajustes de agentes le permiten cambiar los valores de los ajustes de agentes de Traps relacionados con el logging, frecuencia de heartbeat y accesibilidad a la consola. Para obtener más información, consulte Reglas de ajustes de agentes de Traps.
Acción	Las reglas de acción le permiten realizar actividades administrativas en los endpoints. Las acciones de administración de una vez incluyen la desinstalación y actualización de Traps, actualización de licencias, protección del software Traps y borrado de archivos de datos. Para obtener más información, consulte Reglas de acción de Traps.

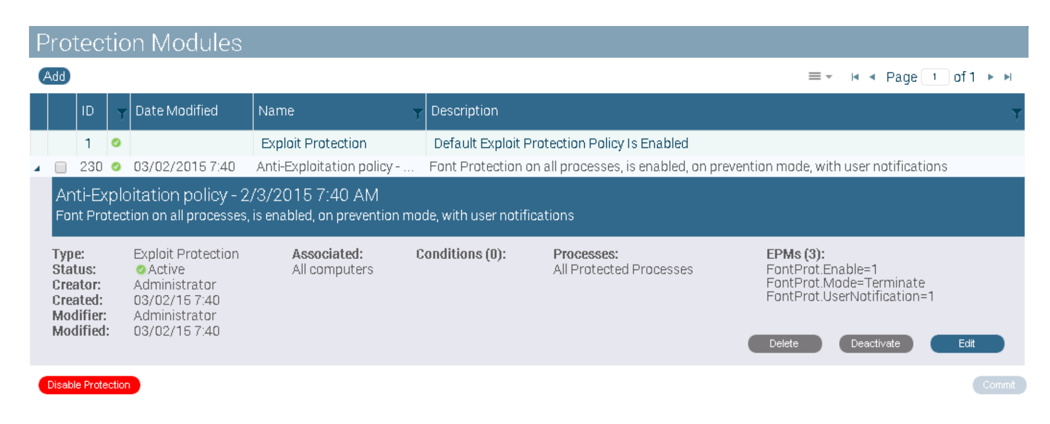
Aplicación de las políticas

El tipo de regla de políticas determina cuándo Traps evalúa la regla. Las reglas de políticas de prevención o restricción de exploits se evalúan solo cuando se activa un proceso o archivo ejecutable que se corresponde con los Objetos de destino, Condiciones y los ajustes que se especifican para la regla. Un objeto de destino puede ser cualquier usuario, grupo, unidad de una organización o equipo que aparece en el Directorio activo o endpoint en el cual se ha instalado Traps. El Endpoint Security Manager identifica los endpoints a través de mensajes que Traps envía al servidor. Una condición puede hacer referencia a una coincidencia exacta de un archivo, un archivo y la versión del archivo, o una ruta de registro que debe existir en el endpoint. También se puede definir una condición para una versión específica de un archivo ejecutable definido en la ruta del archivo.

En intervalos regulares, se envía la política de seguridad más reciente a los endpoints de su red. Puede definir la frecuencia de las actualizaciones de las políticas de seguridad en el endpoint a través del ajuste de heartbeat. También puede recuperar manualmente la política de seguridad más reciente de la consola de Traps. Traps aplica ajustes de agentes o reglas de políticas de acción cuando el endpoint recibe la actualización de la política de seguridad y una regla coincide con los Objetos de destino, Condiciones y los ajustes del endpoint.

Traps evalúa cada una de las reglas de la política de seguridad secuencialmente a través del número de ID: cuanto más alto es el número de ID, mayor es la prioridad de la regla. Se asigna a las reglas creadas o modificadas recientemente un número de ID más alto y, por lo tanto, se evalúan en primer lugar. A diferencia de los cortafuegos de Palo Alto Networks, que evalúan las reglas jerárquicamente, Traps evalúa toda las reglas de las políticas de seguridad de endpoints secuencialmente.

Cada tipo de regla tiene una página de resumen específico de las reglas, que muestra todas las reglas de ese tipo y permite añadir nuevas reglas, ver detalles adicionales acerca de cada regla y realizar tareas de administración de reglas. Desde la página de resumen, también se puede deshabilitar/habilitar la protección para todas las reglas de ese tipo.



Componentes y acciones comunes de las reglas

Cada tipo de regla tiene un conjunto específico de campos obligatorios y opcionales que se pueden personalizar para cumplir con las necesidades de la política de seguridad de la organización.

La tabla siguiente describe los pasos comunes para la creación de una regla de política.

Administración de reglas	Tema
Defina los ajustes y/o acciones específicos para el tipo de regla.	Para más detalles sobre los ajustes específicos necesarios para cada regla, consulte: • Administración de las reglas de protección de exploits • Administración de las reglas de protección de malware • Administración de reglas y ajustes de WildFire • Administración de restricciones en ejecutables • Administración de reglas de acción de Traps • Administración de las reglas de ajustes de agentes • Administración de reglas y ajustes forenses
Añadir condiciones de activación de la regla, es decir, condiciones que el endpoint debe cumplir para una regla.	Condiciones
Definir los objetos de destino (usuarios, equipos, unidades de la organización, grupos y endpoints).	Objetos de destino
Proporcionar un nombre descriptivo para la regla	Nombrar o renombrar una regla
Guardar y opcionalmente activar la regla.	• Guardar reglas • Administración de reglas guardadas
Deshabilitar o habilitar todas las reglas de protección.	Deshabilitar o habilitar todas las reglas de protección.

Condiciones

▲ Definición de condiciones de activación para una regla

▲ Borrado o modificación de una condición de regla

Definición de condiciones de activación para una regla

Las condiciones de activación de reglas son condiciones que debe cumplir el endpoint para la aplicación de una regla en un endpoint. Para cada condición se puede especificar una ruta de archivo ejecutable, una ruta de archivo ejecutable y la versión del archivo, o una ruta de registro que debe existir en el endpoint.

Definición de condiciones de activación para una regla	
Paso 1	Seleccione **Ajustes > Condiciones**. La página **Condiciones** muestra el número de **ID** único, **Nombre**, y **Descripción** para cada condición.
Paso 2	**Añada** una nueva condición.
Paso 3	Introduzca el **Nombre** y **Descripción** de la condición y especifique uno o más de los siguientes ajustes: • **Ruta**—Ruta completa de un archivo ejecutable que existe en el endpoint. • **Ruta de registro**—Ruta completa a una entrada de registro que existe en el endpoint. • **Versión** —Número de versión de un archivo ejecutable que existe en el endpoint y el número de versión del ejecutable. Si se define, también debe especificar la ruta del ejecutable. El ejecutable debe coincidir con la ruta y la versión exacta para la regla que se va a aplicar.
Paso 4	**Guarde** la condición.

Borrado o modificación de una condición de regla

Las condiciones de activación de reglas son condiciones que debe cumplir el endpoint para la aplicación de una regla en un endpoint. Tras crear una condición, puede borrarla o modificarla en la página **Condiciones**.

Modificación o borrado de una condición de regla	
Paso 1	Seleccione **Ajustes > Condiciones**. La página Condiciones muestra el número de **ID** único, **Nombre**, y **Descripción** para cada condición.
Paso 2	Seleccione la condición que desea modificar o borrar.
Paso 3	Proceda con una de las siguientes opciones. • Haga clic en **Borrar** para desechar la condición. • Modifique los ajustes de la condición y **Guarde** los cambios.

Objetos de destino

Los objetos de destino para reglas son los objetos a los que se aplica la regla. Un objeto puede hacer uno de los siguientes:

Objeto de destino	Descripción
Usuario	Un usuario definido en el directorio activo.
Grupo	Un grupo de usuarios definido en el directorio activo.
Equipo	El nombre de un ordenador o un dispositivo móvil definido en el directorio activo.
Unidad organizativa	Una subdivisión en el directorio activo en la que se pueden colocar usuarios, grupos, equipos y otras unidades de la organización.

Objeto de destino	Descripción
Endpoint existente	Un equipo o dispositivo móvil en el que se instala Traps. El Endpoint Security Manager identifica los endpoints existentes a través de mensajes de comunicación enviados desde Traps.

Puede aplicar reglas a todos los objetos de la organización, a objetos seleccionados, o a todos los objetos excepto aquellos de la lista de excluidos.

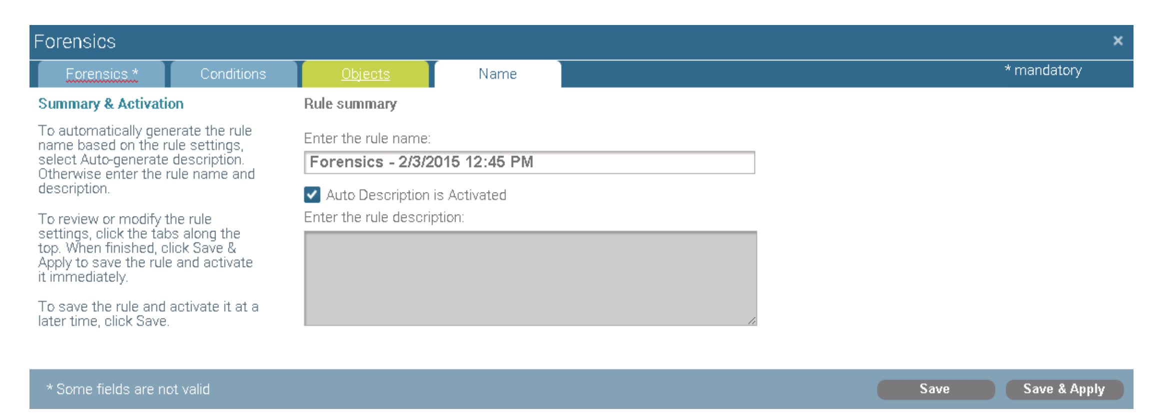
Independientemente del endpoint, las reglas que se definen para usuarios y grupos se aplicarán a esos usuarios y grupos, cualquiera que sea el endpoint en el que inician sesión.

Nombrar o renombrar una regla

La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla y el tiempo de creación. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.

Guardar reglas

Para guardar una regla debe rellenar todos los campos necesarios para ese tipo de regla. Las pestañas con los campos obligatorios se indican con una línea serpenteante bajo el nombre de la pestaña. Rellene los campos obligatorios antes de intentar guardar o modificar una regla.



Tras especificar los campos necesarios para una regla, puede seleccionar una de las acciones siguientes:

Acción	Descripción
Guardar	Guarde la regla sin activarla. El estado de la regla se muestra como **Inactivo** y puede activarse más adelante.
Guardar y aplicar	Guarde la regla y actívela inmediatamente.

Administración de reglas guardadas

Tras guardar la regla, aparecen el nombre y la descripción en diferentes logs del sistema y tablas.

Seleccione la regla para ver los detalles y realizar cualquiera de las acciones siguientes:

Acción	Descripción
Duplicar	(Solo reglas de acción) Crea una nueva regla basada en un modo existente.
Borrar	Borra la regla. La regla se elimina desde el sistema. Para borrar las reglas de una vez, seleccione la casilla de verificación junto a la regla y seleccione **Borrar reglas no por defecto seleccionadas** del menú ≡ ▾ en la parte superior de la tabla.
Activar/Desactivar	Si la regla se ha guardado previamente, pero no se ha aplicado, puede **Activar** la regla para añadirla a la política de seguridad actual. Si la regla está activa, puede **Desactivar** la regla para eliminarla de la política de seguridad actual, pero no borrar la regla del sistema. Para activar/desactivar reglas múltiples de una vez, seleccione la casilla de verificación junto a la regla y seleccione **Activar seleccionado** o **Desactivar seleccionado** del menú ≡ ▾ en la parte superior de la tabla. Para deshabilitar/habilitar todas las reglas de exploits, malware o forenses, consulte Deshabilitar o habilitar todas las reglas de protección..
Editar	Edita la definición de la regla. La selección de esta opción abre el asistente de reglas y le permite cambiar la definición de la regla. Para obtener más información, consulte Creación de una regla de prevención de exploits.
Importar reglas/Exportar seleccionados	En el menú ≡ ▾ de la parte superior de la tabla puede importar reglas o exportar reglas seleccionadas, según sea necesario. La exportación de reglas guarda las reglas seleccionadas en un archivo XML. Para obtener más información, consulte Exportación e importación de archivos de las políticas.

Deshabilitar o habilitar todas las reglas de protección.

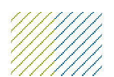
Si la política de seguridad está causando problemas para los endpoints de su organización, puede deshabilitar rápidamente todas las reglas de políticas activas, incluidas las reglas de políticas por defecto.

La deshabilitación de la protección detiene la inyección de Traps en todos los procesos futuros, la validación con respecto a WildFire, posteriores recopilaciones de datos, y elimina efectivamente todas las restricciones. Los cambios en las reglas de seguridad mientras toda la protección está deshabilitada no se harán efectivos hasta que se habilite nuevamente la protección.

Tras deshabilitar la protección e investigar los problemas, puede volver a activar las reglas de políticas habilitando toda la protección La habilitación de la protección no activa las reglas que se han desactivado anteriormente.

En situaciones en las que solo se necesita deshabilitar una regla o un pequeño grupo de reglas, las puede seleccionar individualmente y desactivarlas desde la página de administración de reglas específica para este tipo de regla.

Deshabilitar o habilitar todas las reglas de protección.	
Paso 1	En la consola ESM, seleccione cualquier página de administración de reglas, por ejemplo **Políticas > Malware > Restricciones**.
Paso 2	Para deshabilitar la protección, seleccione **Deshabilitar toda la protección**. El ESM elimina todas las reglas y envía la política de seguridad actualizada a los endpoints en la siguiente comunicación heartbeat con Traps.
Paso 3	Para habilitar la protección, seleccione **Habilitar toda la protección**. El ESM restablece todas las reglas y envía la política de seguridad actualizada a los endpoints en la siguiente comunicación heartbeat con Traps.



Prevención de exploits

Administración de procesos

Por defecto, el Endpoint Security Manager protege los procesos más vulnerables y usados con más frecuencia en entornos de Windows. Se dispone de detalles acerca de estos procesos en la página **Administración de procesos** e incluyen información sobre el tipo de protección, número de ordenadores que ejecutan el proceso, y la fecha y hora en las que se ha descubierto el proceso por primera vez.

Se pueden configurar los procesos como **Protegido**, **Desprotegido**, o **Provisional**. La finalidad del estado **Provisional** es indicar que el proceso está sometido a una *ejecución del informe* como proceso protegido, generalmente en un número reducido de endpoints y un pequeño número de reglas. Una vez finalizada la ejecución y tras realizar los ajustes necesarios a las reglas, puede cambiar el tipo de protección del proceso a **Protegido**.

Con la creación de una regla de ajustes de agentes para recoger información de nuevos procesos, podrá ver los procesos que Traps descubre en los endpoints de su organización. Esto es de utilidad para la detección de procesos no protegidos y su cambio para protegerlos (consulte Recopilación de información de nuevos procesos). También puede añadir protección para otras aplicaciones propias y de terceros sin recoger información de nuevos procesos, añadiéndolos directamente a la lista de procesos protegidos en la página de Administración de procesos.

- Protección de procesos
- Añadir un proceso protegido, provisional o desprotegido
- Importación o exportación de un proceso
- Ver, modificar o borrar un proceso
- Ver procesos actualmente protegidos por Traps

Protección de procesos

Traps protege los siguientes procesos por defecto.

Procesos protegidos por defecto			
7z.exe	explorer.exe	notepad.exe	taskhost.exe
7zFM.exe	filezilla.exe	notepad++.exe	telnet.exe
7zG.exe	firefox.exe	nslookup.exe	unrar.exe
Acrobat.exe	FlashFXP.exe	opera.exe	userinit.exe
AcroRd32.exe	FotoSlate4.exe	opera_plugin_wrapper.exe	vboxservice.exe
acrord32info.exe	foxit reader.exe	OUTLOOK.EXE	vboxsvc.exe
alg.exe	ftp.exe	plugin-container.exe	vboxtray.exe
amp.exe	ftpbasicsvr.exe	POWERPNT.EXE	VISIO.EXE
AppleMobileDeviceService.exe	GoogleUpdate.exe	PPTVIEW.EXE	vlc.exe
APWebGrb.exe	GrooveMonitor.exe	qttask.exe	VPREVIEW.EXE
armsvc.exe	i_view32.exe	QuickTimePlayer.exe	webkit2webprocess.exe
bsplayer.exe	icq.exe	rar.exe	wftp.exe
chrome.exe	ICQLite.exe	reader_sl.exe	winamp.exe
cmd.exe	iexplore.exe	realconverter.exe	winampa.exe
CorelCreatorClient.exe	INFOPATH.EXE	realplay.exe	winrar.exe
CorelCreatorMessages.exe	iPodService.exe	realsched.exe	WINWORD.EXE
ctfmon.exe	itunes.exe	rundll32.exe	winzip32.exe
cuteftppro.exe	iTunesHelper.exe	RuntimeBroker.exe	winzip64.exe
DivX Player.exe	journal.exe	Safari.exe	wireshark.exe
DivX Plus Player.exe	jqs.exe	searchindexer.exe	wmiprvse.exe
DivXConverterLauncher.exe	mirc.exe	skype.exe	wmplayer.exe
DivXUpdate.exe	MSACCESS.EXE	soffice.exe	wmpnetwk.exe
dllhost.exe	msnmsgr.exe	spoolsv.exe	wuauclt.exe
dwm.exe	MSPUB.EXE	svchost.exe	xftp.exe
EXCEL.EXE	netstat.exe	sws.exe	xpsrchvw.exe
	nginx.exe	taskeng.exe	

Añadir un proceso protegido, provisional o desprotegido

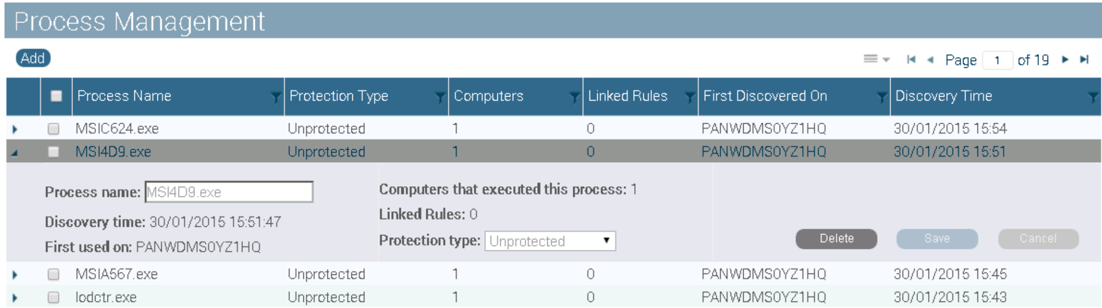
Por defecto, Traps protege las aplicaciones más vulnerables y las que se utilizan con más frecuencia, pero también se pueden añadir a la lista de procesos protegidos otras aplicaciones propias y de terceros. Ampliando la protección a las aplicaciones que son importantes para su organización, puede facilitar la máxima protección con la mínima alteración de las actividades diarias. Añada procesos como protegidos, provisionales o desprotegidos y configúrelos utilizando la página Administración de procesos.



Solo se pueden configurar reglas de prevención de exploits en procesos **Protegidos** o **Provisionales**.



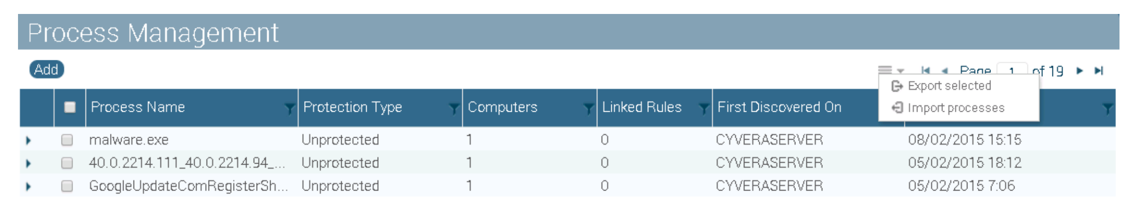
No puede cambiar los procesos **Protegidos** por defecto incluidos en la configuración inicial. Consulte sus dudas al equipo de soporte de Palo Alto Networks.



Añadir un proceso protegido, provisional o desprotegido	
Paso 1 Vaya a la página de Administración de procesos.	En la consola ESM, seleccione **Políticas > Exploit > Administración de procesos**.
Paso 2 Añada un nuevo proceso.	1. Haga clic en **Añadir**. 2. Introduzca el **Nombre de proceso**. 3. Seleccione el **Tipo de protección**: • **Protegido**—Indica que las reglas de seguridad protegen activamente el proceso. • **Provisional**—Le permite separar lógicamente procesos protegidos de los procesos que se están sometiendo a una ejecución del informe como proceso protegido. • **Desprotegido**—Indica que las reglas de seguridad no protegen activamente el proceso.
Paso 3 Guarde los cambios para los procesos protegidos.	Haga clic en **Crear**.

Importación o exportación de un proceso

Utilice las funciones de exportación e importación de la consola Endpoint Security Manager (ESM) para crear una copia de seguridad de una o más definiciones de proceso utilizadas en su política de seguridad.. Las funciones de importación y exportación le permiten hacer copias de seguridad de los procesos antes de la migración o actualización a un nuevo servidor, o antes de implementar un proceso administrado en múltiples servidores independientes. Puede exportar procesos de forma global o individual y guardarlos en un archivo XML. La función de importación agrega los procesos a la lista existente de procesos por defecto y añadidos y muestra sus tipos de protección.



Importación o exportación de un proceso		
Paso 1	Vaya a la página de Administración de procesos.	En la consola ESM, seleccione **Políticas > Exploit > Administración de procesos**
Paso 2	Importe o exporte uno o más procesos.	• Para importar procesos, haga clic en el menú ≡ ▾ y, a continuación, seleccione **Importar procesos**. **Vaya** a los procesos y **Cargue** los que desea importar. Los procesos aparecen en la tabla tras finalizar la carga. • Para exportar procesos, seleccione uno o más procesos que desee exportar. En el menú ≡ ▾, seleccione **Exportar seleccionados**. La consola ESM guarda los procesos en un archivo XML.

Ver, modificar o borrar un proceso

La página de Administración de procesos de la consola Endpoint Security Manager muestra todos los procesos que protege su organización. Para cambiar o borrar un proceso, en primer lugar deberá eliminar el proceso y cualquier regla asociada.

Ver, modificar o borrar un proceso		
Paso 1	Vaya a la página de Administración de procesos.	En la consola ESM, seleccione **Políticas > Exploit > Administración de procesos**

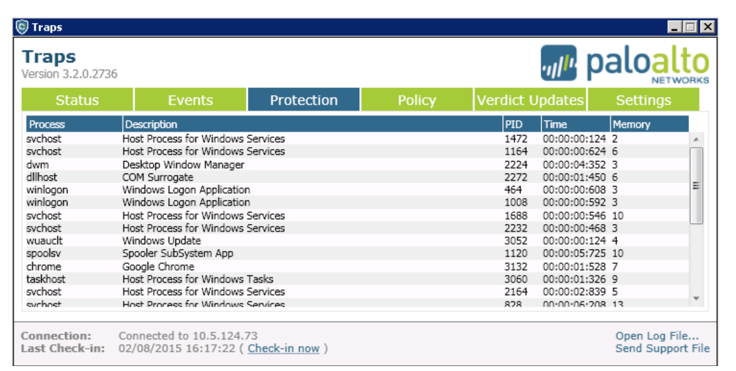
Ver, modificar o borrar un proceso (Continuación)		
Paso 2	Visualice los procesos en la página de Administración de procesos.	Use los controles de la parte superior de la tabla para ver sus diferentes partes. Se muestran los campos siguientes: • **Nombre de proceso**—Nombre de archivo del ejecutable del proceso • **Tipo de protección**—Protegido, desprotegido o provisional • **Ordenadores**—Número de endpoints en el que se ejecuta el proceso • **Reglas vinculadas**—Número de reglas configuradas para el proceso • **Primero descubierto**—Nombre del endpoint en el que se descubrió el proceso por primera vez • **Tiempo de descubrimiento**—Fecha y hora en las que se descubrió el proceso por primera vez en el endpoint (tras recibir una regla para informar de nuevos procesos)
Paso 3	Administre o cambie el proceso.	Seleccione el nombre del proceso, y elija una de las siguientes opciones: • Seleccione **Borrar** para borrar el proceso. • Cambie el **Nombre de proceso** y, a continuación, **Guarde** los cambios. • Cambie el **Tipo de protección** y, a continuación, **Guarde** los cambios.

Ver procesos actualmente protegidos por Traps

Cuando un usuario crea o abre un proceso protegido en el endpoint, Traps inyecta un módulo de protección, conocido como EPM (Exploitation Prevention Module), en el proceso. Las reglas de las políticas de seguridad de endpoints determinan los EPM que se inyectan en cada proceso.

Puede ver los procesos que están protegidos por Traps en al actualidad utilizando la consola de Traps o una interfaz de líneas de comando denominada Cytool (consulte Ver procesos actualmente protegidos por Traps).

La pestaña **Protección** de la consola de Traps muestra los procesos que están protegidos por Traps.



Para cada proceso, Traps muestra el nombre, la descripción, el número de ID único, el tiempo desde el inicio del proceso, y el registro de asignación de memoria.

Ver procesos actualmente protegidos por Traps	
Paso 1	Inicie la consola de Traps: • En la bandeja de Windows, haga clic con el botón derecho en el icono de Traps y seleccione la **Consola**, o haga doble clic en el icono. • Ejecute CyveraConsole.exe desde la pantalla de instalación de Traps. Se inicia la consola de Traps.
Paso 2	Seleccione la pestaña **Avanzada > Protección** para ver los procesos protegidos.

Administración de las reglas de protección de exploits

- ▲ Reglas de protección de exploits
- ▲ Política de prevención de exploits por defecto
- ▲ Creación de una regla de prevención de exploits
- ▲ Exclusión de un endpoint de una regla de prevención de exploits

Reglas de protección de exploits

Una *regla de protección de exploits* utiliza módulos EPM (Exploit Prevention Modules) para proteger los procesos de su organización y controla el comportamiento de los procesos, generalmente bloqueado o permitido. El EPM se dirige a una técnica de exploits específica e inyecta un módulo en el proceso para evitar ataques a las vulnerabilidades de los programas basándose en la corrupción de memoria o fallos lógicos. Un EPM puede proteger al mismo tiempo múltiples aplicaciones y procesos. Los EMP avanzados adicionales están ocultos y solo se puede acceder a ellos en el modo ninja. Los EPM avanzados permiten a los ingenieros de soporte y ventas de Palo Alto Networks configurar ajustes finos adicionales para cada EPM. La tabla siguiente describe los tipos de EPM y el tipo de exploit contra el que puede proteger el módulo:

Nombre	Tipo	Descripción
DEP	Corrupción de memoria.	Prevención de ejecución de datos (DEP). Evita que las áreas de memoria que contienen datos se ejecuten como código ejecutable.
Protección de secuestro de DLL	Fallo lógico de software	Evita ataques de secuestro de DLL en los que el atacante intenta cargar DLL de localizaciones no seguras para obtener el control de un proceso. También evita que el atacante cargue archivos CPL (panel de control) malintencionados.
CPL	Fallo lógico de software	Protege contra vulnerabilidades relacionadas con la rutina de visualización para imágenes de acceso directo del panel de control de Windows, que se pueden usar en la creación de malware.
Seguridad de DLL	Fallo lógico de software	Evita el acceso a metadatos de DLL cruciales de localizaciones de códigos sin confianza.
Comprobación de excepción de Heap Spray	Corrupción de memoria	Detecta instancias de heap sprays cuando ocurren excepciones sospechosas (indicativas de intentos de exploits).
Protección de fuentes	Fallo lógico de software	Evita una manipulación inapropiada de fuentes, un objetivo común de los exploits.
Cookies GS	Fallo lógico de software	Mejora la granularidad de las comprobaciones de seguridad del búfer de Windows para proteger contra el *desbordamiento del búfer*, una técnica de ataque común que explota el código que no aplica las restricciones de tamaño del búfer. Un cambio en el tamaño de la cookie de seguridad que se utiliza para asignar el espacio indica que la pila puede estar desbordada; el proceso se termina si se detecta un valor diferente.

Nombre	Tipo	Descripción
Mitigación de daños en la pila	Corrupción de memoria	Evita que se disparen las vulnerabilidades de daños en la pila, como las de tipo "double free".
Protección de parches activos	Fallo lógico de software	Evita el uso de una nueva técnica que utiliza funciones del sistema para evitar la DEP y la ASLR (Address Space Layout Randomization).
Asignación previa de librería	Fallo lógico de software	Aplica la relocalización de módulos específicos que suelen utilizar los intentos de exploit.
Comprobación de Heap Spray de límite de memoria	Corrupción de memoria	Detecta instancias de heap sprays utilizando nuestro algoritmo exclusivo cuando se produce un incremento repentino en el consumo de memoria (indicativos de exploits en curso).
Protección de desreferencia nula	Corrupción de memoria	Evita que el código malintencionado mapee a dirección cero en el espacio de memoria, haciendo que no se puedan atacar las vulnerabilidades de desreferencia nula.
DLL empaquetadas	Fallo lógico de software	Una extensión del módulo de seguridad DLL; proporciona soporte para DLL empaquetadas que se desempaquetarán en la memoria.
Comprobación periódica de Heap Spray	Corrupción de memoria	Detecta instancias de heap sprays utilizando nuestro algoritmo exclusivo a través del examen de la pila en intervalos de tiempo predefinidos.
Asignación previa aleatoria	Fallo lógico de software	Aumenta la entropía de la disposición de la memoria del proceso para reducir la posibilidad de un ataque de exploits con éxito.
Mitigación de ROP	Corrupción de memoria	Protege contra el uso de la programación orientada al retorno (ROP) protegiendo las API utilizadas en cadenas ROP y de exploits que utilizan los motores de compilación en tiempo de ejecución (KIT).
Protección SEH	Corrupción de memoria	Evita el secuestro del Control de excepciones estructurado (SEH), una estructura de control comúnmente atacada denominada LinkedList, que contiene una secuencia de registros de datos.
Asignación previa de código shell	Fallo lógico de software	Reserva y protege ciertas áreas de memoria de uso común para cargas útiles utilizando técnicas de heap spray.
Protección de ShellLink	Fallo lógico de software	Evita vulnerabilidades lógicas de shell-link.
SYSRET	Fallo lógico de software	Protege contra vulnerabilidades relacionadas con un ataque de escalabilidad de privilegios locales.
UASLR	Fallo lógico de software	Mejora o implementa la ASLR (selección aleatoria de módulos) con mayor entropía, robustez y un estricto cumplimiento.

La política de seguridad por defecto de Endpoint Security Manager contiene reglas de prevención de exploits para un conjunto de procesos de uso común. Para crear reglas de prevención de exploits adicionales, debn configurarse el EPM y los detalles del EPM utilizados para proteger uno o más procesos y, opcionalmente, especificar el Objetos de destino, Condiciones, los procesos, los EPM y las acciones que se deben realizar si se produce un ataque. Un objeto de destino puede ser cualquier usuario, grupo, unidad de una organización o

equipo que aparece en el Directorio activo o endpoint en el cual se ha instalado Traps. El ESM identifica los endpoints a través de mensajes que Traps envía al servidor. Una condición puede hacer referencia a un archivo, un archivo y la versión del archivo, o una ruta de registro que debe existir en el endpoint.

El agente de Traps envía con regularidad la política de seguridad más reciente desde el servidor ESM. Cuando un usuario abre un archivo o URL, el agente de Traps inyecta el EPM en el proceso o procesos relacionados con la apertura del archivo. La política de seguridad determina el tipo de EPM que Traps utiliza para proteger vulnerabilidades o errores del proceso y las acciones que se deben aplicar. Las acciones pueden incluir especificaciones o si debe o no activarse el EPM, terminar el proceso, o informar al usuario acerca del evento de seguridad. Cuando un evento de seguridad activa una regla, el agente de Traps también toma una instantánea de la memoria para la posterior investigación forense.

Encontrará un resumen de las reglas de prevención de exploits en la página **Políticas > Exploit > Módulos de protección**. La selección de una regla de la página muestra información adicional acerca de la regla y otras acciones que se pueden tomar (**Borrar**, **Activar**/**Desactivar**, o **Editar** la regla). Para obtener más información, consulte Administración de las reglas de protección de exploits.



Consulte al soporte de Palo Alto Networks antes de hacer ningún cambio en los EPM en las reglas de políticas de seguridad.

Política de prevención de exploits por defecto

Por defecto, las políticas de seguridad del Endpoint Security Manager continenen Reglas de protección de exploits que se habilitan como protección contra ataques que aprovechan las vulnerabilidades comunes del software y exploits. La tabla siguiente describe los ajustes de las políticas de prevención de exploits por defecto. Para configurar nuevas reglas de prevención de exploits, puede heredar la conducta por defecto que se muestra en la columna Notificación de modo y usuarios, puede anular los ajustes según sea necesario para personalizar la política de seguridad de su organización. Para configurar EPM avanzados, deberá introducir la contraseña de modo ninja.

EPM	Módulo	¿Habilitado por defecto?	Notificación de modo y usuarios	¿Modo ninja?
DEP	G01	✓	Terminar, Notificación=ON	
Seguridad de DLL	DllSec	✓	Terminar, Notificación=ON	
Protección de secuestro de DLL	DllProt		Notificar, Notificación=ON	
Comprobación de excepción de Heap Spray	H02	✓	Terminar, Notificación=ON	
Protección de fuentes	FontProt		Terminar, Notificación=ON	
Genérico	GENÉRICO	✓		✓

EPM	Módulo	¿Habilitado por defecto?	Notificación de modo y usuarios	¿Modo ninja?
Mitigación de daños en la pila	H01	✓	Terminar, Notificación=ON	
Protección de parches activos	B01		Terminar, Notificación=ON	
Asignación previa de librería	P02	✓	Terminar, Notificación=ON	
SEH principal	SEH principal	✓		✓
VEH principal	VEH principal	✓		✓
Comprobación de Heap Spray de límite de memoria	T02	✓	Terminar, Notificación=ON	
Protección de desreferencia nula	K01	✓	Terminar, Notificación=ON	
DLL empaquetadas	PACKED_DLL	Lista vacía por defecto	Terminar=ON	
Comprobación periódica de Heap Spray	D01		Terminar, Notificación=ON	
Mitigación de ROP	R01		Terminar, Notificación=ON	
Protección SEH	S01	✓	Terminar, Notificación=ON	
Asignación previa de código shell	P01	✓	Terminar, Notificación=ON	
Protección de ShellLink	ShellLink	✓	Terminar, Notificación=ON	
T01 Compatibilidad	T01	✓	Terminar, Notificación=ON	✓
UASLR	UASLR	✓	Terminar, Notificación=ON	
Protección URI	URI			✓

Creación de una regla de prevención de exploits

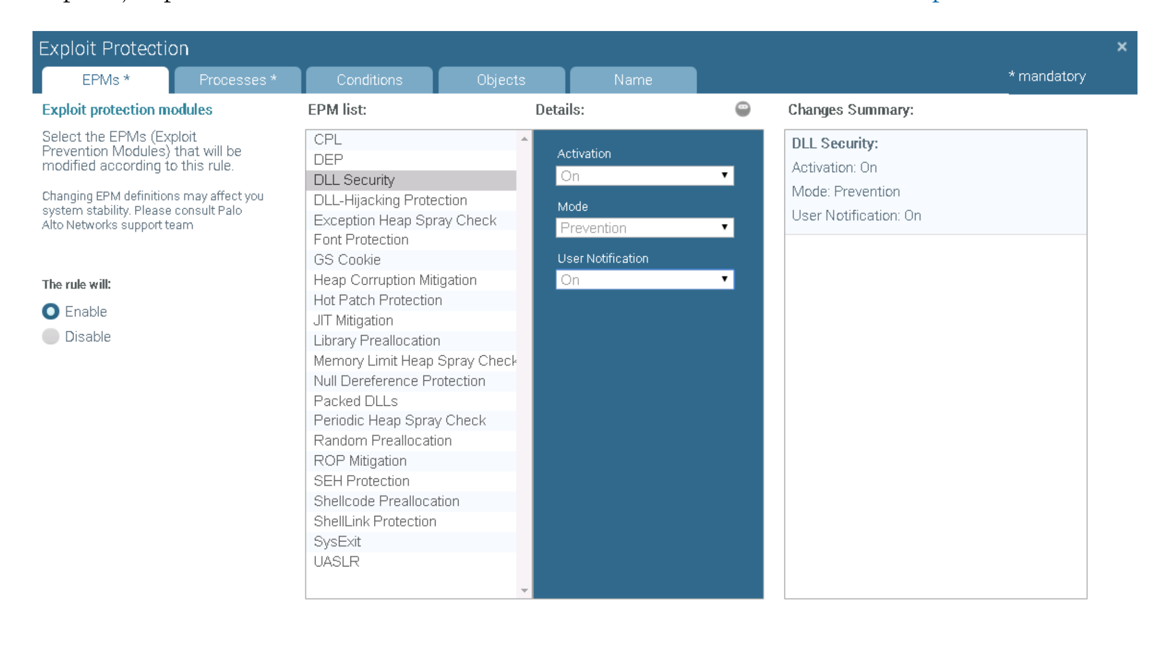
Cree una regla de prevención de exploits para definir el módulo específico utilizado para proteger los procesos utilizados con más frecuencia en su organización. Cada módulo evita intentos de exploits en las vulnerabilidades de los programas basados en la corrupción de la memoria o fallos lógicos y protege contra un método de ataque específico, por ejemplo, secuestro de DLL o daños en la pila. Puede configurar un módulo para proteger uno o más procesos que puedan ser vulnerables a ese tipo de ataque.

Por defecto, Traps protege los procesos utilizados con más frecuencia usando reglas de prevención de exploits preconfiguradas. Para una lista de procesos protegidos por la política de seguridad por defecto, consulte Protección de procesos. Las reglas de prevención de exploits por defecto no se pueden modificar. Para anular el comportamiento de las reglas de prevención de exploits por defecto, cree una nueva regla para administrar ese proceso.



La configuración de reglas de prevención de exploits es una característica avanzada. Para cambiar o anular una regla de prevención de exploits, consulte al equipo de soporte de Palo Alto Networks.

Antes de configurar una regla de prevención de exploits o un nuevo proceso, debe definir el proceso y el tipo de protección en la página **Políticas > Exploit > Administración de procesos**. Para añadir un nuevo proceso, consulte Añadir un proceso protegido, provisional o desprotegido. Para cambiar el tipo de protección de un proceso, por ejemplo de **Desconocido** a **Protegido**, consulte Ver, modificar o borrar un proceso.



Creación de una regla de prevención de exploits		
Paso 1	Inicie una nueva regla de prevención de exploits.	Seleccione **Políticas > Exploit > Módulos de protección** y, a continuación, **Añada** una nueva regla.

Creación de una regla de prevención de exploits (Continuación)		
Paso 2	Configure los detalles del EPM.	1. **Habilitar** o **Deshabilitar** la inyección de módulos de prevención de exploits (EPM) en los procesos seleccionados. 2. Para habilitar uno o más EPM, seleccione el EPM de la lista y configure sus ajustes en la sección Detalles. Los ajustes de cada tipo de EPM son diferentes, pero pueden incluir preferencias sobre si terminar o no un proceso e informar a un usuario acerca de un evento de seguridad. Repita el proceso para añadir más EPM. Para obtener más información sobre los diferentes tipos de EPM, consulte Reglas de protección de exploits. ! El cambio de las definiciones de los EPM puede afectar a su nivel de protección y cambia el orden en el que se evalúan las reglas (consulte Aplicación de las políticas). Para no comprometer la seguridad de su organización, consulte al equipo de soporte de Palo Alto Networks.
Paso 3	Seleccione el proceso para el que que desea aplicar la regla.	1. Seleccione la pestaña **Procesos**. 2. Reduzca la lista de procesos seleccionando el tipo de proceso en el menú desplegable, **Protegido** o **Provisional**. Los procesos provisionales son aquellos que se están sometiendo a una ejecución del informe y se monitorizan por separado de los procesos protegidos. 3. Seleccione uno o más procesos a los que se aplicará la regla y, a continuación, haga clic en **Añadir**. O, para aplicar la regla a todos los procesos protegidos o provisionales, seleccione, **Todos los procesos**.
Paso 4	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 5	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 6	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.

Creación de una regla de prevención de exploits (Continuación)		
Paso 7	Guarde la regla de prevención de exploits.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la norma más adelante, seleccione la regla en la página **Políticas > Exploit > Módulos de protección** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Exploit > Módulos de protección**. Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Exclusión de un endpoint de una regla de prevención de exploits

Cuando un endpoint intenta lanzar una aplicación que incumple la política de prevención de exploits, el agente de Traps detiene el proceso de ejecución e informa del proceso malintencionado a la consola Endpoint Security Manager. La página **Eventos de seguridad > Amenazas** proporciona información detallada acerca de los procesos que activan eventos de seguridad y el Exploit Prevention Modules (EPMs) que evita los ataques.

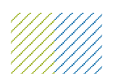
Para permitir que el proceso se ejecute en un endpoint específico sin borrar o deshabilitar la regla de políticas, cree una regla de exclusión según los detalles de los eventos de seguridad. La definición de una regla de exclusión deshabilita el EPM que evitaba la ejecución del proceso en un endpoint específico.



Para evitar la exposición de forma innecesaria de su organización a los ataques, cree reglas de exclusión solo cuando sea necesario.

También puede crear reglas de exclusión para uno o más objetos de la organización (consulte Creación de una regla de prevención de exploits).

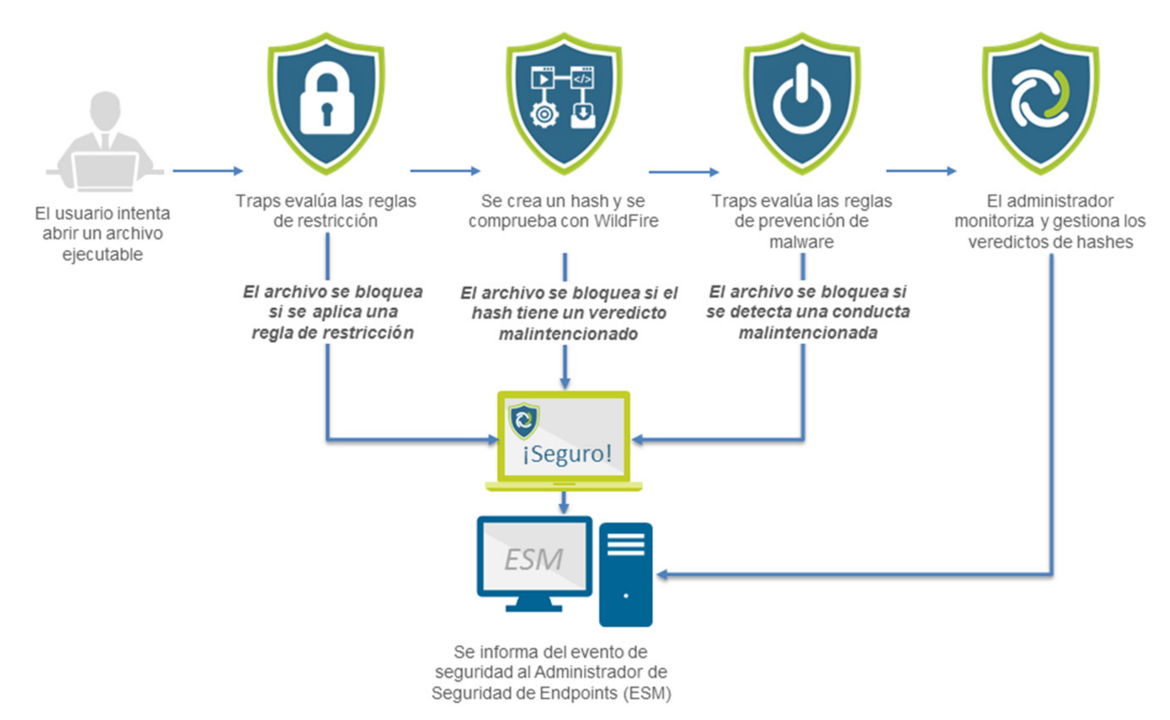
Exclusión de un endpoint de una regla de prevención de exploits		
Paso 1	Lance la página Amenazas.	En la consola ESM, seleccione **Eventos de seguridad, Amenazas > Threats**.
Paso 2	Seleccione el evento.	Seleccione el evento de seguridad para el que que desea crear la regla de exclusión. El evento se expande para mostrar detalles y acciones adicionales en relación con el evento de seguridad.
Paso 3	Cree una regla de exclusión.	1. Haga clic en **Crear** para poblar la regla con detalles relacionados con el EPM y el endpoint específicos. El botón solo está disponible para reglas de prevención de exploits. 2. Si es necesario, revise los detalles en las pestañas **Procesos**, **Condiciones**, **Objetos** y **Nombre**. 3. **Guarde y aplique** la regla inmediatamente o **Guarde** la regla para activarla más adelante.
Paso 4	Verifique que la regla de exclusión permite la ejecución del proceso en el endpoint.	1. Abra la consola de Traps. 2. Seleccione **Registrar ahora** para solicitar la política de seguridad más reciente. 3. Seleccione **Avanzado > Política** y verifique que aparece la regla. 4. Lance la aplicación en el endpoint para verificar que el usuario puede ejecutar el proceso con éxito.



Prevención de malware

Flujo de prevención del malware

El motor de prevención del malware se centra en tres métodos principales de prevención: reglas de políticas de restricción que examinan la fuente del archivo, módulo de prevención del malware que se centran en las conductas con frecuencia iniciadas por procesos maliciosos, y el análisis de WildFire.



- Fase 1: Evaluación de las políticas de restricción
- Fase 3: Evaluación de las políticas de prevención de malware
- Fase 2: Evaluación de veredictos de hashes
- Fase 4: Administración de veredictos

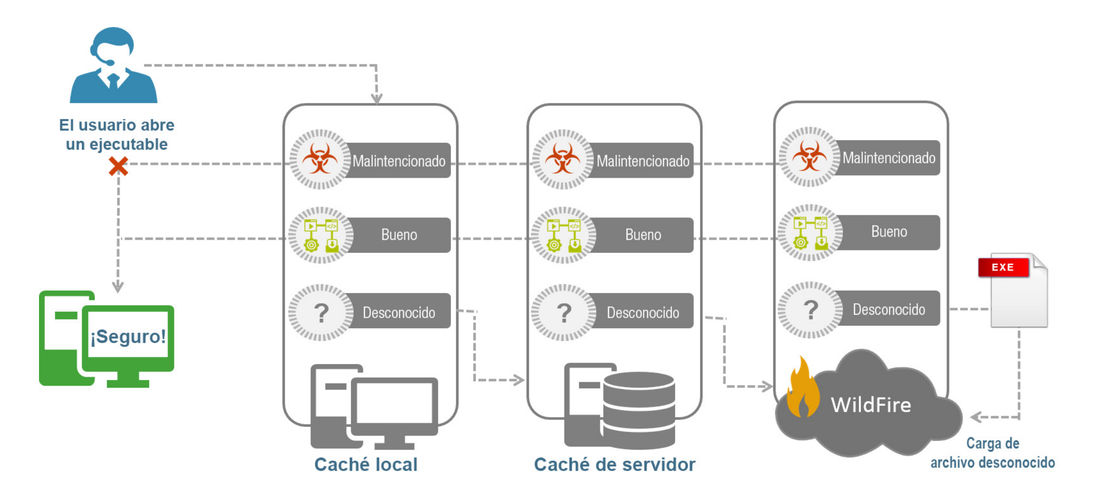
Fase 1: Evaluación de las políticas de restricción

Cuando un usuario o máquina intenta abrir un ejecutable, Traps verifica en primer lugar que el ejecutable no viole ninguna regla de restricción. Por ejemplo, puede haber reglas de restricción que bloquean archivos ejecutables no firmados o que bloquean ejecutables abiertos desde localizaciones de red. Si se aplica alguna de las reglas de restricción al ejecutable, Traps bloquea la ejecución del archivo e informa del evento de seguridad al Endpoint Security Manager.

Dependiendo de la configuración de cada regla de restricción, Traps también puede informar al usuario sobre el evento de prevención.

Si no se aplica ninguna regla de políticas de restricciones al ejecutable, Traps evalúa a continuación las reglas que protegen contra el malware, según se describe en Fase 3: Evaluación de las políticas de prevención de malware.

Fase 2: Evaluación de veredictos de hashes



Cuando se habilita WildFire (consulte Habilitación de WildFire), Traps crea un hash único para cada archivo ejecutable que un usuario o máquina intentan abrir. Traps realiza entonces una consulta en su caché local para determinar si el hash corresponde a una decisión oficial, conocida como *Veredicto de WildFire* y si el archivo es malintencionado o benigno. Si el hash no se corresponde con un veredicto del caché local, Traps hace una consulta al servidor ESM. Si el servidor ESM no tiene un veredicto para el hash, el servidor ESM hace una consulta a WildFire. Las etapas de evaluación se describen de forma más detallada en las secciones siguientes:

- Búsqueda de caché local (en el endpoint)
- Búsqueda en el caché del servidor (en el servidor ESM)
- Búsqueda en WildFire

Búsqueda de caché local (en el endpoint)

Cuando un usuario abre un archivo ejecutable, Traps crea un hash único para el archivo y realiza una búsqueda de veredicto en su caché local. El caché local se guarda en la carpeta C:\ProgramData\Cyvera\LocalSystem en el endpoint y contiene los hashes y los veredictos correspondientes para cada archivo que un usuario o máquina intenta abrir en el endpoint. El caché se escala en tamaño para acomodar el número de archivos ejecutables únicos que se han abierto en el endpoint. Cuando se habilita la protección del servicio (consulte Gestión de protección de servicios) los hashes solo son accesibles a través de Traps y no se pueden cambiar.

Si el veredicto asociado con el hash indica que el archivo es benigno, Traps permite la ejecución del archivo. Si el veredicto asociado con el hash es malintencionado, Traps informa del evento de seguridad a Endpoint Security Manager. A continuación, dependiendo de la conducta de terminación configurada para archivos malintencionados, Traps realiza una de las acciones siguientes:

- Bloquea el ejecutable malintencionado
- Informa al usuario acerca del archivo, pero sigue permitiendo la ejecución del archivo
- Realiza un log del problema sin notificarlo al usuario y permite la ejecución del archivo.

Si el hash no existe en el caché local o tiene un veredicto desconocido, Traps consulta al servidor ESM para ver si el hash tiene un veredicto correspondiente en el caché del servidor.

Búsqueda en el caché del servidor (en el servidor ESM)

Tras recibir una solicitud de veredicto de hash, el servidor ESM realiza una búsqueda en su caché de servidor. El caché del servidor contiene veredictos para todos los archivos ejecutables que se han abierto en todos los endpoints de su organización.

Si la búsqueda de hashes devuelve un veredicto malintencionado o benigno, el servidor ESM comunica el veredicto a Traps en la siguiente comunicación heartbeat. Si el archivo resulta ser benigno, Traps permite al usuario abrir el ejecutable. Si el archivo es malintencionado, Traps realiza un log del evento de seguridad y gestiona el archivo según la política de seguridad para archivos malintencionados (generalmente, el bloqueo).

Si el valor hash del caché del servidor es desconocido o el hash no se corresponde con un veredicto conocido, el servidor ESM hace una consulta a WildFire.

Búsqueda en WildFire

WildFire guarda veredictos para cada uno de los archivos enviados y/o analizados por WildFire. El servidor ESM consulta a WildFire cada 30 minutos, o en un intervalo preconfigurado según sus preferencias, para obtener veredictos de hash para archivos cuyos veredictos son desconocidos en el caché del servidor.

Si WildFire devuelve un veredicto que indica que un archivo es benigno o malintencionado, el servidor ESM actualiza su caché del servidor. A continuación, en la siguiente comunicación heartbeat con Traps, el servidor ESM comunica el veredicto a cualquier endpoint en el que un usuario ha intentado abrir el archivo ejecutable.

Si WildFire devuelve un veredicto desconocido (WildFire no ha analizado el archivo previamente), puede configurar el servidor ESM para el envío automático del ejecutable desconocido (hasta 100 MB cada uno) a WildFire para su análisis. Cuando WildFire ha analizado el archivo, guarda el veredicto en su base de datos y devuelve ese veredicto en consultas posteriores acerca del hash desconocido.



Si la carga automática de archivos desconocidos está deshabilitada (por defecto), puede seleccionar manualmente archivos individuales para su envío a WildFire y su posterior análisis. Para habilitar la carga automática de archivos desconocidos, consulte Habilitación de WildFire.

Si no es posible acceder a WildFire, el servidor ESM recoge el veredicto del hash como **Sin conexión** y comunica el veredicto en la siguiente comunicación con Traps.

Dependiendo de la conducta configurada para archivos desconocidos, archivos sin conexión, y archivos malintencionados de su política de seguridad, Traps bloquea el archivo o permite su apertura al usuario. Cuando Traps realiza las acciones asociadas con el veredicto del archivo ejecutable, se pueden mantener los hashes y sus veredictos según se describen en Fase 3: Evaluación de las políticas de prevención de malware.

Fase 3: Evaluación de las políticas de prevención de malware

Si WildFire borra el ejecutable, Traps permite la ejecución del archivo. Si el ejecutable muestra una conducta malintencionada, Traps detiene la ejecución del archivo y evita que continúe la conducta malintencionada. Por ejemplo, se puede tener una regla de inyección de subprocesos que evita la creación de subprocesos remotos. Si el ejecutable lanza e intenta crear subprocesos remotos, Traps bloquea la ejecución del archivo e informa del evento de seguridad al Endpoint Security Manager.

Si no se aplica ninguna regla de políticas de prevención del malware al ejecutable y WildFire está habilitado, Traps cambia a Fase 4: Administración de veredictos.

Fase 4: Administración de veredictos

Puede revisar los veredictos de hashes para los archivos ejecutables de su organización y buscar hashes específicos en la página **Políticas > Malware > Control de hashes** (consulte Vista y búsqueda de hashes).

- Actualizaciones automáticas de veredictos
- Actualizaciones manuales de veredictos

Actualizaciones automáticas de veredictos

WildFire guarda veredictos para cada uno de los archivos enviados y/o analizados por WildFire. Según WildFire recibe y analiza nuevas muestras del Equipo de inteligencia de subprocesos de Palo Alto Networks y de los clientes de WildFire, actualiza su base de datos expansiva de hashes y veredictos.

Para mantener un caché actualizado de hashes y veredictos de WildFire, el servidor ESM consulta periódicamente a WildFire los cambios en los veredictos, por ejemplo, de benignos a malintencionados. El servidor ESM consulta a WildFire, en lotes de hasta 500 hashes únicos, en relación con archivos desconocidos una vez cada 30 minutos y también consulta a WildFire acerca de archivos malintencionados y benignos conocidos cuyo veredicto ha cambiado en los últimos 30 días. La consulta de cambios en los veredictos de archivos conocidos se ejecuta cada 1440 minutos (24 horas). Utilice la consola ESM para cambiar la frecuencia de consultas y cambiar el número de días en los que WildFire debe volver a buscar veredictos cambiados.

Actualizaciones manuales de veredictos

Puede obtener un informe WildFire detallado para cada archivo ejecutable, benigno o malintencionado, analizado por WildFire (consulte Visualización de informes de WildFire). El informe contiene información de archivos, un resumen de conducta acerca del ejecutable, y detalles sobre la red y la actividad del host.

Utilice la información del informe de WildFire para ayudarle a decidir si cancelar o revocar un veredicto. La anulación de un veredicto solo cambia el veredicto para una archivo específico en el caché del servidor y no afecta a WildFire o su política de seguridad global (consulte Anulación de una decisión de WildFire). Tras cambiar el veredicto del hash a malintencionado o benigno, la consola ESM muestra el veredicto cambiado en la página **Control de hashes**. La cancelación permanece activa hasta que la elimina el administrador, momento en el que vuelve al último veredicto conocido por el servidor ESM.

Para forzar al servidor ESM a comprobar de nuevo un veredicto con WildFire, puede revocar el hash utilizando la consola ESM (consulte Revocación de una decisión de WildFire). El servidor ESM consulta inmediatamente a WildFire la obtención del veredicto actual acerca del hash. Cuando WildFire devuelve el veredicto, el servidor ESM actualiza el caché del servidor, y comunica el veredicto a cualquier endpoint o endpoints que han intentado previamente abrir el archivo ejecutable en la siguiente comunicación heartbeat con Traps.

El servidor ESM comunica cualquier cambio en el veredicto, por ejemplo, una actualización desde WildFire o una cancelación manual, a cualquier endpoint que haya abierto previamente el archivo en la siguiente comunicación heartbeat con Traps.

Administración de restricciones en ejecutables

Las reglas de restricción le permiten definir limitaciones o excepciones sobre el modo en que se gestionan los ejecutables en los endpoints de su red.

Reglas de restricción

Con frecuencia, los atacantes ocultan archivos ejecutables malintencionados o se incluyen como embedidos en archivos no malintencionados. Causan daños en los equipos al intentar obtener el control, al recopilar información confidencial o al interrumpir las operaciones normales del sistema. La tabla siguiente muestra *reglas de restricción* que se pueden configurar para limitar o colocar excepciones sobre el modo en que se gestionan los ejecutables en su red:

Reglas de restricción	Descripción
Ejecución de ejecutables provenientes de carpetas concretas	Muchos escenarios de ataques se basan en la escritura de archivos ejecutables malintencionados en ciertas carpetas y su ejecución. Generalmente, es aconsejable restringir el acceso a carpetas locales *temp* y de *descarga* y a carpetas de red. Para hacer una excepción en la restricción general, puede permitir carpetas específicas. Para más información, consulte Administración de listas blancas globales, Carpetas locales no permitidas, Lista blanca de carpetas de red.
Ejecución de ejecutables provenientes de medios externos	El código malintencionado puede acceder a endpoints a través de medios externos, como unidades de disco desmontables y discos ópticos. Como medida de protección, se pueden definir restricciones sobre la ejecución de ejecutables de discos externos en los endpoints de su red. Para obtener más información, consulte Definición de restricciones y excepciones de medios externos.
Procesos que diseminan procesos secundarios	Un código malintencionado se puede activar y legitimar procesos para diseminar procesos secundarios malintencionados. Bloquee el código malintencionado definiendo una regla de restricción apropiada. Para obtener más información, consulte Definición de restricciones y excepciones de procesos secundarios.

Reglas de restricción	Descripción
Procesos de Java que se ejecutan desde los navegadores	Un punto de entrada común para códigos malintencionados son los procesos de Java importados desde un host remoto y ejecutados bajo los navegadores de Internet. Como protección contra estos exploits, evite que un applet de Java ejecute objetos bajos los navegadores, al tiempo que se permite la ejecución de ciertos procesos de confianza. Puede elegir selectivamente las acciones permitidas (lectura, escritura o ejecución) de los tipos de archivos de proceso, localizaciones y rutas de registro. Para obtener más información, consulte Definición de restricciones y excepciones de Java.
Ejecución de procesos sin firmar	Un proceso *firmado* tiene una firma de autenticación digital que prueba su procedencia de una fuente de confianza. Las prácticas correctas dictan que todas las aplicaciones legítimas deben tener una firma, pero no siempre se cumplen. Las restricciones sobre procesos sin firma evitan la ejecución de todos los procesos no firmados, excepto aquellos permitidos explícitamente. También puede definir un *periodo de aplazamiento*, que evita la ejecución de procesos sin firma durante un plazo de tiempo determinado tras su escritura en el disco del endpoint. Debido a que un ataque puede incluir la escritura de un ejecutable malintencionado en el disco y su ejecución inmediata, la utilización de un periodo de aplazamiento y la restricción de procesos sin firma son medios efectivos para prevenir ataques de malware. Para obtener más información, consulte Definición de restricciones y excepciones de ejecutables sin firma.

Para cada restricción se especifica el objeto u objetos de destino, la condición o condiciones, el tipo de restricción y la acción o acciones que deben realizarse para la administración de ejecutables. Un objeto de destino puede ser cualquier usuario, grupo, unidad de una organización o equipo que aparece en el Directorio activo o endpoint en el cual se ha instalado Traps. El ESM identifica los endpoints a través de mensajes que Traps envía al servidor. Una condición puede hacer referencia a un archivo, un archivo y la versión del archivo, o una ruta de registro que debe existir en el endpoint.

Cuando un usuario intenta abrir un ejecutable, el agente de Traps evalúa las reglas de restricción (si las hay) que deben aplicarse al archivo y realiza las acciones asociadas. La acción determina si el agente de Traps evitará o no la ejecución del archivo, e informará al usuario cuando se active una regla de restricción.

Puede crear o editar reglas de restricción en el resumen **Restricciones** y la página de administración (**Políticas > Malware > Restricciones**). La selección de una regla muestra información adicional acerca de la regla y otras acciones que se pueden tomar (**Borrar**, **Activar**/**Desactivar**, o **Editar** la regla). Para obtener más información, consulte Administración de restricciones en ejecutables.

Añadir una nueva regla de restricción

Cree una nueva regla de restricción para definir limitaciones sobre el modo en que los ejecutables se ejecutan en los endpoints.

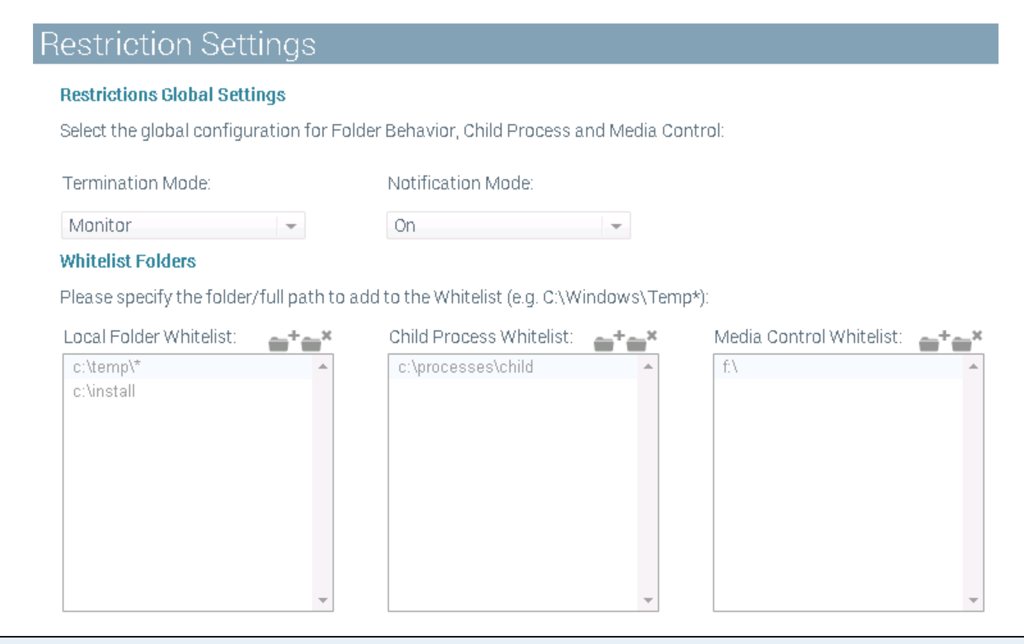
Añadir una nueva regla de restricción		
Paso 1	Inicie una nueva regla restricción.	Seleccione **Políticas > Malware > Restricciones** y **Añadir** una nueva regla.

Añadir una nueva regla de restricción (Continuación)		
Paso 2	Seleccione el tipo de regla de restricción que desea añadir.	Seleccione uno de los siguientes y configure los ajustes según el tipo de restricción: • **Conducta de carpetas locales**—Para más información, consulte Carpetas locales no permitidas. • **Conducta de carpetas de red**—Para más información, consulte Lista blanca de carpetas de red. • **Medios externos**—Para más información, consulte Definición de restricciones y excepciones de medios externos. • **Procesos secundarios**—Para más información, consulte Definición de restricciones y excepciones de procesos secundarios. • **Java**—Para más información, consulte Definición de restricciones y excepciones de Java. • **Ejecutables sin firma**—Para más información, consulte Definición de restricciones y excepciones de ejecutables sin firma.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de restricción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > Restricciones** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Restricciones.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Administración de listas blancas globales

Para permitir la ejecución de ejecutables de carpetas locales y medios externos y permitir el inicio de procesos secundarios de procesos principales de una carpeta específica, puede configurar una lista blanca global. De forma similar a la funcionalidad de listas blancas existente para procesos de Java, ejecutables sin firma e inyección de subprocesos, se pueden especificar rutas completas y variables de rutas y también comodines para coincidencias de patrones (**%** para la coincidencia de términos similares y ***** para la coincidencia de cero o más caracteres).

Los elementos de la sección de la lista blanca tienen prioridad sobre cualquier elemento no permitido y se evalúan en primer lugar en la política de seguridad.



Administración de listas blancas globales	
Paso 1	En la consola ESM, seleccione **Políticas > Exploit > Ajustes de restricción**.
Paso 2	Para especificar si Traps debe o no bloquear el ejecutable cuando se abre desde localizaciones no incluidas en la lista blanca, configure el **Modo de terminación**: • **Monitor**—No bloquea el acceso a ejecutables y procesos, sino realiza un log cuando se abren los archivos desde localizaciones que no están en la lista blanca e informa de los eventos al ESM. • **Prevenir**—Bloquea los ejecutables y procesos.
Paso 3	Para especificar si Traps debe o no informar al usuario cuando el ejecutable se abre desde una localización no incluida en la lista blanca, configure el **Modo de notificación**: • **On**—Se notifica al usuario. • **Off**—No se notifica al usuario.
Paso 4	Haga clic en el icono Añadir carpeta situado junto a las áreas de listas blancas de Carpeta local, Proceso secundario o Control de medios e introduzca la ruta de la carpeta, por ejemplo `C:\Windows\Temp*`.
Paso 5	Haga clic en **Confirmar**. Puede volver a la página **Ajustes de restricción** en cualquier momento para modificar los ajustes de listas blancas globales.

Carpetas locales no permitidas

Muchos escenarios de ataques se basan en la escritura de archivos ejecutables malintencionados en ciertas carpetas como “temp” y “descarga” y la ejecución de los ejecutables. Se puede restringir el acceso a carpetas locales comunes añadiendo la carpeta a una lista negra. Cuando un usuario intenta abrir un ejecutable de una carpeta no permitida, Traps bloquea el intento e informa del evento de seguridad al ESM. Para hacer una excepción en la restricción general, añada una carpeta a una lista blanca (consulte Administración de listas blancas globales).

Carpetas locales no permitidas		
Paso 1	Inicie una nueva regla restricción.	Seleccione **Políticas > Malware > Restricciones** y **Añadir** una nueva regla.
Paso 2	Defina la conducta de la carpeta local.	1. Seleccione **Conducta de carpeta local** en la lista desplegable **Restricciones**. 2. Para bloquear la ejecución de ejecutables de carpetas locales, seleccione la casilla de verificación, haga clic en el icono Añadir carpeta y añada la ruta de la carpeta a la sección Lista negra. 3. Repita según sea necesario para añadir carpetas múltiples.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de restricción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > Restricciones** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Restricciones.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Lista blanca de carpetas de red

Para evitar escenarios de ataque basados en la escritura de ejecutables malintencionados en carpetas remotas, puede crear una regla de restricción de conducta de carpetas de red que define las localizaciones de red permitidas para las que se pueden ejecutar ejecutables. Cuando un usuario intenta abrir un ejecutable de una carpeta que no se ha especificado en la regla de restricción, Traps bloquea el intento e informa del evento de seguridad al ESM.

Lista blanca de carpetas de red		
Paso 1	Inicie una nueva regla restricción.	Seleccione **Políticas > Malware > Restricciones** y **Añadir** una nueva regla.
Paso 2	Defina la conducta de la carpeta de red.	1. Seleccione **Conducta de carpeta de red** en la lista desplegable **Restricciones**. 2. Para permitir la ejecución de ejecutables de carpetas de red específicas, seleccione la casilla de verificación, haga clic en el icono Añadir carpeta y añada la ruta de la carpeta a la sección Lista negra. 3. Repita según sea necesario para añadir carpetas múltiples.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de restricción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > Restricciones** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Restricciones.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Definición de restricciones y excepciones de medios externos

El código malintencionado puede acceder a endpoints a través de medios externos, como unidades de disco desmontables y discos ópticos. Como medida de protección, se pueden definir reglas de restricción que evitan la ejecución de ejecutables de unidades de disco externas conectadas a los endpoints. La definición de una restricción en medios externos protege contra cualquier intento para la ejecución de un ejecutable desde una unidad de disco externa.

Definición de restricciones y excepciones de medios externos		
Paso 1	Inicie una nueva regla restricción.	Seleccione **Políticas > Malware > Restricciones** y **Añadir** una nueva regla.
Paso 2	Defina la conducta de restricción para medios externos. Por defecto, se permite la ejecución de aplicaciones no malintencionadas y desconocidas de discos desmontables y ópticos.	1. Seleccione **Medios externos** en la lista desplegable **Restricciones**. 2. Seleccione la casilla de verificación para el tipo de medio externo del que se desea evitar la ejecución de aplicaciones. • **Discos desmontables** • **Discos ópticos**
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de restricción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > Restricciones** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Restricciones.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Definición de restricciones y excepciones de procesos secundarios

En un intento de controlar un endpoint, un atacante puede hacer que un proceso legítimo genere un proceso secundario malintencionado. Defina una regla de restricción para evitar que procesos secundarios sean activados desde uno o más procesos.

Definición de restricciones y excepciones de procesos secundarios		
Paso 1	Inicie una nueva regla restricción.	Seleccione **Políticas > Malware > Restricciones** y **Añadir** una nueva regla.
Paso 2	Defina la conducta de restricción para los procesos secundarios. Por defecto, se permiten los procesos secundarios generados desde un proceso protegido.	1. Seleccione **Procesos secundarios** en la lista desplegable **Restricciones**. 2. Seleccione el tipo de **Procesos** que desea restringir, **Protegido** para mostrar procesos que protege activamente la política de seguridad, o **Provisional y Desprotegido** para mostrar procesos que están sometidos a una ejecución del informe y procesos que no están activamente protegidos por la política de seguridad. 3. Seleccione uno o más procesos de la lista, los que no deberán generar procesos secundarios, y haga clic en **Añadir**. El proceso o procesos seleccionados aparecen en la lista Procesos seleccionados. Mientras selecciona, mantenga pulsada la tecla **CTRL** para seleccionar múltiples procesos. Para modificar las listas de procesos, consulte Administración de procesos.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de restricción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > Restricciones** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Restricciones**. Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Definición de restricciones y excepciones de Java

Un punto de entrada común para códigos malintencionados son los procesos de Java importados desde un host remoto y ejecutados bajo los navegadores de Internet. Como medida de protección contra estos exploits, se puede evitar que un applet de Java ejecute objetos bajo los navegadores. Alternativamente, puede permitir la ejecución de procesos de confianza. Utilice la opción para elegir de forma selectiva los tipos de archivos, localizaciones y rutas de registro que pueden leer estos procesos y en los que pueden escribir.

Definición de restricciones y excepciones de Java		
Paso 1	Inicie una nueva regla restricción.	Seleccione **Políticas > Malware > Restricciones** y **Añadir** una nueva regla.
Paso 2	Defina las restricciones en los procesos de Java. Por defecto, las restricciones de procesos de Java están deshabilitadas. La habilitación de los ajustes EPM de Java le permite poner restricciones en los procesos de Java, pero no habilita o deshabilita ninguna de las reglas de EPM.	1. Seleccione **Java** en la lista desplegable **Restricciones**. 2. Seleccione **Habilitar EPM de Java** en las opciones **Ajustes de EPM de Java**. 3. En la sección Procesos permitidos de Java, haga clic en el botón para especificar los procesos de Java cuya ejecución se permitirá desde el navegador, por ejemplo `AcroRd32.exe`. Repita esta acción para añadir procesos adicionales. 4. Para especificar si un proceso de Java puede modificar ajustes de registros, seleccione **Habilitado** en la lista desplegable **Modificaciones de registro**, y configure los permisos de registro: a. Para cada ruta de registro, ajuste los permisos **Leer**, **Escribir**, y **Borrar** en **Permitir**, **Bloquear**, o **Heredar** (por defecto) según sea necesario. b. Haga clic en el botón para añadir cualquier ruta de registro adicional. 5. Para especificar si un proceso de Java puede leer o escribir un archivo, seleccione **Habilitado** en la lista desplegable **Modificaciones del sistema de archivos**, y configure los permisos de archivos: a. Para cada nuevo patrón de archivos, ajuste los permisos de escritura o lectura en **Permitir**, **Bloquear**, o **Heredar** (por defecto) según sea necesario. b. Haga clic en el botón para agregar un nuevo patrón de archivos. 6. En la lista **Navegadores**, seleccione o deseleccione los navegadores en los que se implementa la protección de Java.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.

Definición de restricciones y excepciones de Java (Continuación)		
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de restricción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > Restricciones** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Restricciones.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Definición de restricciones y excepciones de ejecutables sin firma

Un proceso *firmado* tiene una firma de autenticación digital que prueba su procedencia de una fuente de confianza. Las prácticas correctas dictan que todas las aplicaciones legítimas tenga firma. Las restricciones sobre procesos sin firma evitan la ejecución de todos los procesos sin firma, excepto aquellos permitidos explícitamente. También puede definir un *periodo de aplazamiento*, que evita la ejecución de procesos sin firma durante un plazo de tiempo determinado tras su escritura en el disco del endpoint. Debido a que un ataque puede incluir la escritura de un ejecutable malintencionado en el disco y su ejecución inmediata, la utilización de un periodo de aplazamiento y la restricción de procesos sin firma son medios efectivos para prevenir ataques de malware.

Definición de restricciones y excepciones de ejecutables sin firma		
Paso 1	Inicie una nueva regla restricción.	Seleccione **Políticas > Malware > Restricciones** y **Añadir** una nueva regla.

(Continuación)Definición de restricciones y excepciones de ejecutables sin firma (Continuación)		
Paso 2	Defina las restricciones en los ejecutables sin firma.	1. Seleccione **Ejecutables sin firma** en la lista desplegable **Restricciones**. 2. Introduzca un número de minutos en el campo **Periodo de lista negra** para evitar que los procesos sin firma se ejecuten dentro de este intervalo tras la escritura del archivo ejecutable en el disco del endpoint. 3. Para permitir la ejecución inmediata de un proceso, sin esperar un número definido de minutos, añada el proceso a **Procesos permitidos** haciendo clic en . 4. Para permitir la ejecución inmediata de todos los procesos de una determinada carpeta, sin esperar un número definido de minutos, añada el proceso a la lista **Procesos permitidos** haciendo clic en .
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de restricción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > Restricciones** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Restricciones.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Administración de reglas y ajustes de WildFire

- Habilitación de WildFire
- Reglas de WildFire
- Configuración de una regla de WildFire

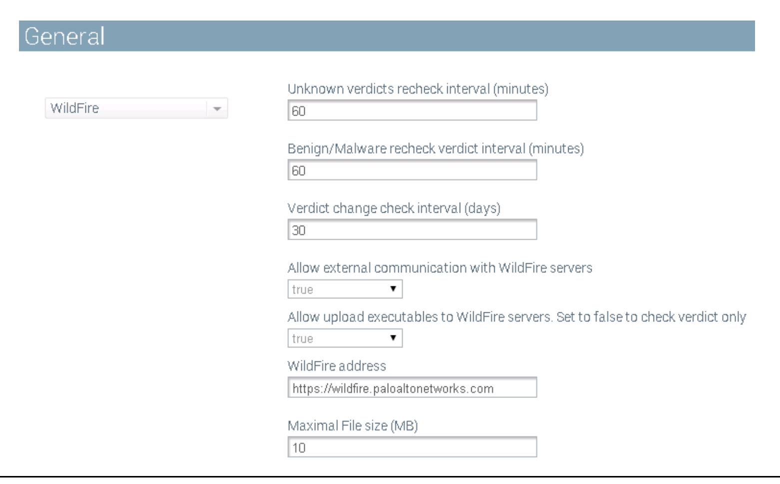
Habilitación de WildFire

WildFire es la solución de análisis de Palo Alto Networks para el análisis de archivos desconocidos, incluidos ejecutables desconocidos utilizando un dispositivo WildFire local o la nube WildFire. WildFire contiene veredictos para todos los archivos examinados: benigno en el caso de un archivo seguro, o malintencionado en el caso del malware. La integración de WildFire con Traps es un servicio opcional que integra análisis WildFire en la solución de endpoints de Traps.

Cuando un usuario o máquina intenta abrir un archivo ejecutable en el endpoint, Traps crea un identificador único (conocido como *hash*) y lo comprueba con la base de datos de WildFire. Si WildFire confirma que un archivo es malware conocido, el agente de Traps bloquea el archivo e informa al ESM (para más información, consulte Administración de hashes ejecutables). De forma predeterminada, la integración de WildFire está deshabilitada.

Habilitación de WildFire

Paso 1 En la consola ESM, seleccione **Ajustes > General > Amenazas**.



Paso 2 Introduzca en minutos la frecuencia con la que el servidor ESM reenvía hashes a WildFire para archivos desconocidos. Un archivo puede tener un veredicto desconocido si es la primera vez que un endpoint envía el hash al servidor o si WildFire no ha analizado todavía el archivo. Por defecto son 30 minutos y debe tener un valor entre uno y 20.160 minutos.

Paso 3 Introduzca los minutos de la frecuencia con la que el servidor ESM vuelve a comprobar el valor de hashes conocidos benignos o maltencionados con WildFire. Por defecto son 1.440 minutos (24 horas) y debe tener un valor entre uno y 20.160 minutos.

Habilitación de WildFire (Continuación)	
Paso 4	Por defecto, (cada 24 horas o según se especifique en Paso 3) el servidor ESM consulta a WildFire para determinar cuáles de los veredictos (si los hay) han cambiado en los últimos 30 días. Para cambiar cuánto retroceden las consultas de cambios del servidor ESM, seleccione un valor entre uno y 30 días y el campo **Intervalo de comprobación de cambios de veredictos**. Por ejemplo, si se especifica un valor de 15, significa que el servidor ESM consultará veredictos que hayan cambiado durante los últimos 15 días.
Paso 5	Habilitación de ajustes de WildFire: • Seleccione **Permitir comunicación externa con servidores WildFire: verdadero** para permitir que el ESM verifique hashes con WildFire. • Seleccione **Permitir cargar ejecutables en servidores WildFire: verdadero** para permitir que el ESM envíe archivos para su análisis en WildFire. Seleccione la opción **falso** para verificar solamente veredictos.
Paso 6	Introduzca la dirección web del servidor WildFire, dispositivo WF-500 local o la nube WildFire (https://wildfire.paloaltonetworks.com), que se utilizará para comprobar hashes y archivos.
Paso 7	Por defecto, el servidor ESM envía archivos de hasta 10MB a WildFire para su análisis. Para cambiar el tamaño máximo de archivo, introducir un valor entre uno y 100MB. No se enviarán a WildFire, de forma automática o manual, los archivos que superen el tamaño máximo.

Reglas de WildFire

Configure las *reglas de WildFire* para hacer un ajuste fino de la conducta y preferencias relacionadas con el análisis de archivos ejecutables para diferentes grupos de Objetos de destino. Un objeto de destino puede ser cualquier usuario, grupo, unidad de una organización e equipo que aparece en el Directorio activo o cualquier endpoint en el cual se ha instalado Traps. El ESM identifica los endpoints a través de mensajes que Traps envía al servidor.

Para cada regla WildFire, puede configurar ajustes de envío de archivos desconocidos a WildFire para su análisis, especificar si Traps informará al usuario acerca de ejecutables malintencionados, especificar la conducta de Traps cuando no hay comunicación con el servidor o con WildFire, y configurar la conducta de Traps cuando WildFire no reconoce un proceso. Puede crear o editar reglas de WildFire en el resumen **Restricciones** y la página de administración (**Políticas > Malware > WildFire**). La selección de una regla muestra información adicional acerca de la regla y otras acciones que se pueden tomar (**Borrar**, **Activar**/**Desactivar**, o **Editar** la regla).

Para obtener más información, consulte Habilitación de WildFire.

Configuración de una regla de WildFire

Cuando se habilita WildFire, Traps crea un hash único para cada ejecutable y verifica el estado del archivo con WildFire. La configuración de reglas de WildFire le permite realizar un ajuste fino de las preferencias y habilitar la funcionalidad para diferentes objetos de destino. Para cada regla WildFire, puede configurar ajustes de envío de archivos desconocidos a WildFire para su análisis, especificar si Traps informará al usuario acerca de ejecutables malintencionados, especificar la conducta de Traps cuando no hay comunicación con el servidor o con WildFire, y configurar la conducta de Traps cuando WildFire no reconoce un proceso.

Configuración de una regla de WildFire		
Paso 1	Verifique que WildFire está habilitado.	Consulte Habilitación de WildFire.
Paso 2	Inicie una nueva regla de WildFire.	1. Seleccione **Políticas > Malware > WildFire**. 2. **Añada** una nueva regla o seleccione y **Edite** una regla existente.
Paso 3	(Opcional) Configure los ajustes de WildFire. Por defecto, WildFire hereda la conducta de la política por defecto. Para cancelar los ajustes, configure los ajustes de WildFire para cumplir con las necesidades de su organización.	1. A la izquierda, **Deshabilite** o **Habilite** la integración de WildFire. La habilitación de la integración de WildFire permite a Traps crear y comprobar veredictos de hash frente a su caché local de hashes. 2. Para habilitar que el agente de Traps cargue archivos desconocidos en el servidor ESM, seleccione **Habilitado** en la lista desplegable **Carga de ejecutables**. 3. Seleccione el **Modo de terminación**, la conducta de Traps cuando WildFire confirma que un archivo ejecutable es malintencionado. • Seleccione **Heredar** para usar la conducta definida por la política por defecto (la política por defecto se utiliza para el modo de aprendizaje). • Seleccione **Terminar** para bloquear el ejecutable malintencionado. • Seleccione **Notificar** para permitir que el usuario abra el ejecutable, haga un log del problema e informe al usuario. • Seleccione **Aprendizaje** para permitir que el usuario abra un ejecutable malintencionado y haga un log del problema, pero sin informar al usuario. 4. En la lista desplegable **Notificación al usuario**, especifique si Traps informará al usuario acerca del ejecutable seleccionando **On** u **Off**. 5. Seleccione una de las siguientes opciones del cambio **Sin conducta de comunicación** para especificar lo que debe hacer el endpoint si no puede llegar al servidor ESM o WildFire. Por defecto, Traps intenta consultar a WildFire cada 2 horas (120 minutos). • Seleccione **Continuar**para permitir la apertura de un archivo ejecutable si Traps no puede llegar al servidor ESM o WildFire para verificar la seguridad del archivo. • Seleccione **Terminar**para bloquear un archivo ejecutable si Traps no puede llegar al servidor ESM o WildFire para verificar la seguridad del archivo. 6. Seleccione la **Conducta de proceso desconocido**, la conducta de Traps cuando WildFire no reconoce un proceso. • Seleccione **Continuar** para permitir que un usuario abra un ejecutable desconocido. • Seleccione **Terminar** para bloquear un ejecutable desconocido.

Configuración de una regla de WildFire (Continuación)		
Paso 4	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 5	(Opcional) Defina el Objetos de destino al que se aplica la regla de WildFire.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 6	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 7	Guarde la regla de WildFire.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware > WildFire** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas de WildFire aparecen en la página **Políticas > Malware > WildFire.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Administración de hashes ejecutables

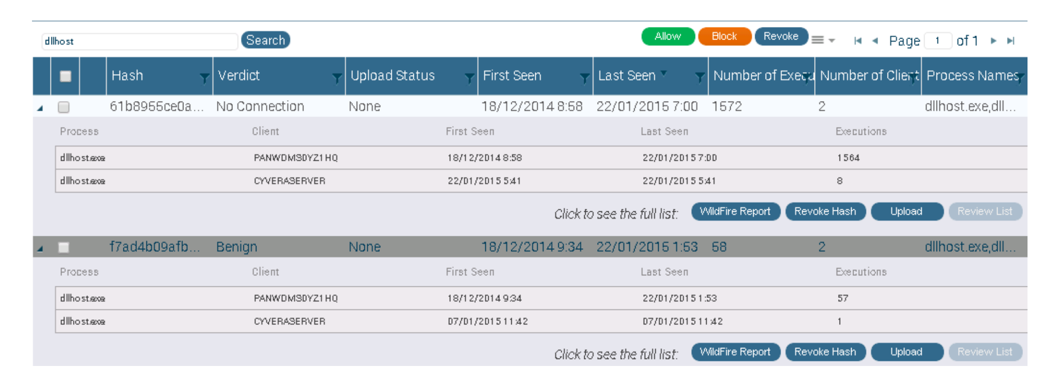
Cuando se habilita la integración de WildFire, Traps crea un hash único para archivos ejecutables ejecutados en un endpoint y lo comprueba con WildFire. La página **Control de hashes** muestra la respuesta de WildFire para cada hash enviado a WildFire.

Si WildFire ya ha analizado un ejecutable y ha determinado que es malware, responde que el ejecutable es **Malintencionado**. Si WildFire ya ha analizado un ejecutable y ha determinado que no contiene un código o conducta malintencionados, WildFire responde que el ejecutable es **Benigno**. Si WildFire no ha analizado previamente el ejecutable, responde que el estado del archivo es **Desconocido**. Si el servidor ESM no llega al WildFire, el estado del archivo se marca como **Sin conexión**. Especifique las acciones asociadas con veredictos malintencionados, benignos, desconocidos y sin conexión en los ajustes de integración de WildFire (consulte Habilitación de WildFire).

- Vista y búsqueda de hashes
- Visualización de informes de WildFire
- Anulación de una decisión de WildFire
- Revocación de una decisión de WildFire
- Carga de un archivo en WildFire para su análisis

Vista y búsqueda de hashes

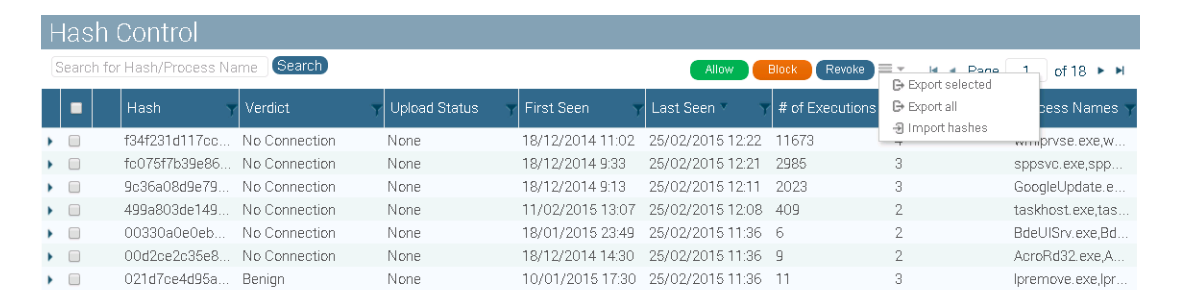
La página **Control de hashes** muestra una tabla de todos los hashes ejecutables de los que han informado los agentes de Traps de su organización y sus veredictos. Un campo de búsqueda en la parte superior de la página le permite filtrar los resultados por cadenas completas o parciales. La búsqueda consulta los valores de hashes y los nombres de procesos y devuelve cualquier resultado coincidente. Los hashes son únicos, mientras los nombres de procesos se pueden incluir más de una vez.



Exportación e importación de hashes

La página **Control de hashes** muestra información acerca de los hashes y los veredictos que se asocian con todos los archivos ejecutables y los usuarios y/o máquinas que han intentado abrir en su organización. Puede hacer una copia de seguridad periódicamente de uno o más hashes exportando el registro o registros a un archivo

XML. La exportación del registro o registros de los hashes también puede ser de utilidad ante de migrar o actualizar a un nuevo servidor. La importación de los registros de hashes añade cualquier hash nuevo a la tabla de control de hashes existente.



Exportación e importación de archivos de hashes

Paso 1 En la consola ESM, seleccione **Políticas > Malware > Control de hashes**.

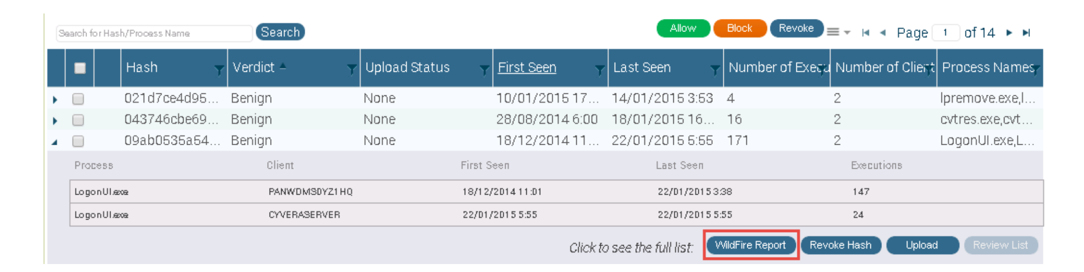
Paso 2 Proceda con una de las siguientes opciones:

- Exportación de registros de hashes:
  - Para exportar todos los registros, seleccione el menú ≡ ▾ de la parte superior de la tabla y, a continuación, seleccione **Exportar todos**.
  - Para exportar uno o más registros, seleccione la casilla de verificación junto al registro o registros. A continuación, en el menú ≡ ▾ de la parte superior de la tabla, seleccione **Exportar seleccionados**.

  El Endpoint Security Manager guarda las reglas seleccionadas en un archivo XML.
- Para restaurar o importar nuevas reglas de políticas, seleccione **Importar hashes**en el ≡ ▾ menú de la parte superior de la tabla. Vaya al archivo de políticas, y haga clic en **Cargar**.

Visualización de informes de WildFire

El ESM guarda los informes de WildFire que contienen un resumen de conducta para cualquier archivo ejecutable que WildFire ha analizado previamente. El informe de WildFire está disponible en PDF e incluye información que se puede usar para decidir si cancelar o no la decisión de WildFire para un archivo ejecutable.

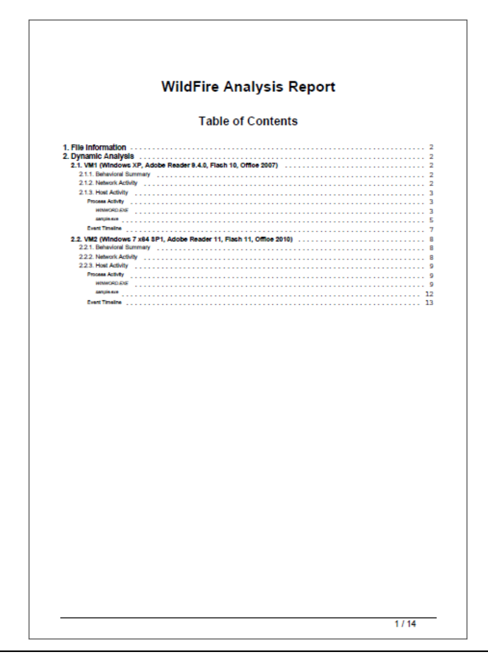


Visualización de informes de WildFire desde la consola ESM

Paso 1 En la consola ESM, seleccione **Políticas > Malware > Control de hashes**.

Paso 2 Busque y seleccione el hash para el que le gustaría ver el informe.

Visualización de informes de WildFire desde la consola ESM (Continuación)	
Paso 3	Haga clic en **Obtener informe**. La consola ESM muestra el informe de caché.



WildFire Analysis Report

Table of Contents

1 / 14

Anulación de una decisión de WildFire

Puede cancelar localmente una decisión de WildFire para permitir o bloquear un archivo sin que afecte al veredicto de WildFire. Esto puede ser de utilidad cuando se necesita crear una excepción para un archivo específico sin alterar la política de seguridad global. Tras cancelar el veredicto, la consola ESM muestra cualquier cambio en el veredicto de WildFire en la página de control de hashes. La cancelación permanece activa hasta su eliminación, momento en el que vuelve al último veredicto conocido por el servidor.

Por ejemplo, considere un caso en el que WildFire devuelve un veredicto sobre un hash específico e indica que el archivo es desconocido. Si su política de seguridad está configurada para bloquear todos los archivos desconocidos y usted cree que el archivo es benigno, puede cancelar la política para permitir la ejecución de un archivo específico sin alterar la política global. Más tarde, si WildFire devuelve un nuevo veredicto que indica que el archivo ha sido analizado y se ha determinado que es malintencionado, verá la notificación en la página de control de hashes. En ese caso, puede eliminar la cancelación y permitir que política de seguridad bloquee el archivo malintencionado.

Gestión de las decisiones de WildFire		
Paso 1	Cancelación de la decisión local de WildFire para un hash.	1. En la consola ESM, seleccione **Políticas > Malware > Control de hashes**. 2. (Opcional) Introduzca el hash o el nombre del proceso en el cuadro de búsqueda y pulse Intro. 3. Seleccione el hash de proceso. Para cancelar el veredicto de WildFire, haga clic en **Permitir** para permitir la ejecución del archivo o **Bloquear** para bloquear la ejecución de un archivo.

Gestión de las decisiones de WildFire (Continuación)		
Paso 2	Visualice los cambios de veredictos de WildFire para tomar decisiones sobre si se elimina o no una cancelación local.	En intervalos preconfigurados, el servidor ESM sondea WildFire para ver si el veredicto ha cambiado para algún hash que se ha guardado en esta base de datos. Revise con regularidad los cambios en el veredicto en la página **Política > Malware > Control de hash** de la consola ESM.
Paso 3	Eliminación de una cancelación local para un veredicto de WildFire.	Las decisiones de cancelación se agrupan para permitir decisiones (el veredicto se sobrescribe para permitir la ejecución del archivo), y bloquear decisiones (el veredicto se sobrescribe para bloquear la ejecución del archivo). 1. En la consola ESM, seleccione **Políticas > Malware > Cancelar veredictos**. 2. Seleccione uno o más hashes de proceso, y haga clic en **Deshacer** para volver al último veredicto en el servidor.

Override Verdicts

Processes manually set to allow — Undo — Page 1 of 1

Hash	Process Names	WildFire Verdict	Last Seen	Number of Clients
5fdcf73191bff9dbb03886755ffcf0bc15849f...	taskeng.exe,taskeng.exe	Unknown	24/01/2015 5:01	2

Revocación de una decisión de WildFire

Para forzar una inmediata recomprobación de un veredicto, revoque el hash en el servidor ESM. Esto sirve de ayuda cuando se sospecha que WildFire ha cambiado el veredicto de un archivo y quiere forzar al servidor ESM a consultar en WildFire el veredicto actualizado. Tras recibir la respuesta de WildFire, el servidor ESM actualiza el caché del servidor. A continuación, en la siguiente comunicación heartbeat con Traps, el servidor ESM comunica el veredicto a cualquier endpoint en el que un usuario ha intentado abrir el archivo ejecutable.

Revocación de una decisión de WildFire	
Paso 1	En la consola ESM, seleccione **Políticas > Malware > Control de hashes**.
Paso 2	Para visualizar el veredicto de WildFire para un hash específico, proceda con una de las opciones siguientes: • Utilice la búsqueda de la parte superior de la página para buscar un valor de hash o nombre de proceso. • Utilice los controles de paginado de la parte superior derecha de cada página para ver diferentes partes de la tabla.
Paso 3	Seleccione la fila para ver detalles adicionales acerca del hash de proceso, y proceda siguiendo una de estas opciones: • Seleccione **Revisar lista** para ver todas las instancias de un hash de proceso. La opción está disponible cuando hay cinco o más instancias de un hash de proceso. • Seleccione **Revocar hash** para volver a consultar el veredicto para el hash con WildFire.

Carga de un archivo en WildFire para su análisis

Antes de la integración de la solución de protección avanzada del endpoint, normalmente WildFire solo analizaba un ejecutable si se enviaba o se cargaba desde el cortafuegos, o si se enviaba usando el portal de WildFire. Esto significaba que algunos ejecutables, aunque comunes, podían no ser analizados previamente porque no era común enviarlos utilizando métodos tradicionales. Para reducir el número de archivos ejecutables desconocidos para el servidor ESM y WildFire, se puede enviar de forma manual o automática el archivo a WildFire para su análisis inmediato. Para enviar archivos desconocidos a WildFire, consulte Habilitación de WildFire.

Si se deshabilita la opción de envía automático de archivos desconocidos, puede cargar manualmente un archivo, caso por caso. Cuando un usuario abre un ejecutable desconocido, Traps carga el archivo, que no debe exceder el tamaño máximo configurado, a la carpeta forense. A continuación, cuando se inicia una carga manual del archivo, el servidor ESM envía el archivo desde la carpeta forense a WildFire.

Cuando WildFire completa su análisis y devuelve el veredicto y el informe, el servidor ESM envía el veredicto cambiado a todos los agentes de Traps e implementa la política.

Según crece el número de agentes que habilitan el envío automático de archivos desconocidos o que se envían manualmente, se espera que el número total de archivos desconocidos se reduzca significativamente para todos los usuarios.

Carga de un archivo en WildFire para su análisis	
Paso 1	En la consola ESM, seleccione **Políticas > Malware > Control de hashes**.
Paso 2	Para visualizar el veredicto de WildFire para un hash específico, proceda con una de las opciones siguientes: • Utilice la búsqueda de la parte superior de la página para buscar un valor de hash o nombre de proceso. • Utilice los controles de paginado de la parte superior derecha de cada página para ver diferentes partes de la tabla. • Para filtrar las entradas de la tabla, haga clic en el icono del filtro a la derecha de la columna para especificar hasta dos conjuntos de criterios para la filtración de los resultados. Por ejemplo, filtre la columna Veredicto para archivos desconocidos.
Paso 3	Seleccione la fila para ver detalles adicionales acerca de hash del proceso, y **Cargue** el archivo en WildFire.

Administración de las reglas de protección de malware

Las reglas de prevención de malware le permiten restringir la conducta relacionada con el malware. Cuando se habilitan, estos módulos utilizan un modelo de listas blancas que permite la inyección de procesos solo a los procesos especificados en la política. Las políticas de prevención de malware por defecto que vienen preconfiguradas con el software ESM conceden excepciones a procesos legítimos comunes que deben inyectarse en otros procesos y/o módulos.

Cuando se añaden nuevas reglas de prevención de malware a la política de seguridad, el mecanismo de reglas de Traps aúna todas las reglas configuradas en una política efectiva que se evalúa para cada endpoint. En el caso de un potencial conflicto entre dos o más reglas, existe un conjunto de consideraciones, como la fecha de modificación, que determina cuál de las reglas se hace efectiva. En otras palabras, la regla editada/creada más recientemente tiene prioridad sobre la regla más antigua. Como resultado, cualquier nueva regla de prevención de malware puede cancelar la política por defecto que hace que no sea efectiva y/o causa una inestabilidad en un endpoint. Además, las listas blancas definidas por los usuarios no se fusionan entre diferentes reglas y se evalúan solo si la regla tiene prioridad.



Tenga cuidado a la hora de configurar nuevas reglas de políticas de prevención de malware para evitar la cancelación de la política por defecto, lo que causará inestabilidad en el sistema operativo.

Para más información acerca de la configuración de reglas de prevención de malware, póngase en contacto con el equipo de soporte o su ingeniero de ventas.

Para evitar la cancelación accidental de la política por defecto, recomendamos la configuración de nuevas reglas solo en procesos que no estén cubiertos por la política por defecto. Cuando se configura una nueva regla, se puede habilitar la protección del módulo de malware para el proceso principal y usar los ajustes de la política por defecto o personalizar las ajustes de reglas para su organización. Para realizar cambios en la política de seguridad para procesos que ya están protegidos, recomendamos importar y cambiar las políticas por defecto, según sea necesario para adecuarlas a su política de seguridad, como describe en los flujos de trabajo siguientes:

- Reglas de prevención de malware
- Configuración de protección de inyección de subprocesos
- Configuración de la protección de suspensión

Reglas de prevención de malware

Una *regla de prevención de malware* evita la ejecución de malware, con frecuencia disimulado o embedido en archivos no malintencionados, utilizando módulos de malware dirigidos a conductas de procesos comunes activadas por el malware.

A diferencia de las reglas de prevención de exploits, que son de inclusión voluntaria (se habilitan los módulos para los procesos específicos que se desean proteger), las reglas de prevención de malware son de exclusión voluntaria (se habilitan los módulos para proteger procesos y especificar el proceso o procesos permitidos para realizar la conducta definida).

Puede habilitar la inyección de módulos de prevención de malware en todos los procesos o habilitar la protección en uno o más procesos protegidos de su organización. Para permitir la ejecución de procesos legítimos, puede crear una lista blanca de procesos principales que se inyectan en otros procesos. También se

dispone de opciones adicionales de listas blancas en el modo ninja . Los ajustes avanzados de listas blancas permiten a los ingenieros de soporte y ventas de Palo Alto Networks configurar ajustes finos adicionales para cada módulo de malware.

La siguiente tabla describe los módulos de prevención de malware:

Reglas de prevención de malware	Descripción
Protección de suspensión	Protege contra una técnica de malware común en la que el atacante crea procesos en un estado suspendido, para inyectar y ejecutar el código antes de iniciarse el proceso. Se puede habilitar la protección de suspensión en un modo de proceso fuente y se puede configurar la notificación del usuario, y opcionalmente permitir módulos de función que pueden llamar a procesos secundarios. Para obtener más información, consulte Configuración de la protección de suspensión.
Inyección de subprocesos	El código malintencionado también puede entrar creando subprocesos y procesos remotos. Puede habilitar la inyección de subprocesos para detener la creación de subprocesos y procesos remotos y especificar la limitación en la fuente o en el proceso o subproceso de destino. Admita carpetas específicas para hacer excepciones en la regla de restricción general. Para obtener más información, consulte Configuración de protección de inyección de subprocesos.

Configuración de protección de inyección de subprocesos

Un proceso puede incluir uno o más subprocesos que ejecutan cualquier parte del código de proceso. Algunos escenarios de ataques se basan en la inyección de un código malintencionado en un proceso objetivo para crear subprocesos remotos, mantener la persistencia y controlar el sistema infectado.

La política por defecto contiene reglas diseñadas para evitar la creación de subprocesos remotos malintencionados y permite procesos legales que deben inyectar subprocesos en otros procesos. Las reglas de políticas por defecto para la inyección de subprocesos suelen almacenarse en la carpeta C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Web\KnowledgeBase\Malware modules\ThreadInjection, pero puede ser diferente si se ha especificado una localización alternativa para la instalación. Visualice los archivos de esta carpeta para determinar si existe un archivo base de política de inyección de subprocesos para el proceso.



Tenga cuidado a la hora de configurar nuevas reglas de inyección de subprocesos para evitar la cancelación de la política por defecto, lo que causará inestabilidad en el sistema operativo.

Para más información acerca de la configuración de reglas de prevención de malware, póngase en contacto con el equipo de soporte o su ingeniero de ventas.

Si el proceso no está ya protegido por la política de seguridad por defecto, puede crear una nueva regla que habilite la protección de inyección de subprocesos para un proceso que utilice los ajustes de inyección de subprocesos por defecto o puede configurar los ajustes según sea necesario para su política de seguridad. Los ajuste incluyen el nombre del proceso, **Activación de módulos** (**Habilitar** o **Deshabilitar**), **Modo de proceso fuente** (**Terminar** o **Notificar**), **Notificación al usuario** (**On** u **Off**), y permitir procesos objetivo a los que se puede inyectar el proceso fuente.

Si el proceso ya está protegido por la política de seguridad por defecto, recomendamos importar la inyección de subprocesos por defecto como nueva regla y realizar cambios para adecuarla a su organización. De este modo, cuando se activa la política, cancela la política por defecto pero sigue conteniendo los ajustes de configuración por defecto, además de los cambios realizados.

Configuración de protección de inyección de subprocesos		
Paso 1	(Opcional) Importe una copia de la política por defecto. Esto es necesario solo para procesos que ya están protegidos por la configuración por defecto y evita que se sobrescriba la política por defecto.	1. Seleccione **Políticas > Malware > Módulos de protección**. 2. En el menú , seleccione **Importar reglas**. 3. **Vaya** a los archivos de políticas por defecto de la carpeta Traps para acceder al proceso fuente deseado, y haga clic en **Cargar**. La regla importada aparece en la tabla de las reglas de prevención de malware.
Paso 2	Inicie o modifique una regla de prevención de malware.	**Añada** una nueva regla o seleccione y **Edite** una regla existente.
Paso 3	Habilite la protección de inyección de subprocesos para un proceso individual o para todos los procesos.	1. Seleccione **Inyección de subprocesos** en la lista desplegable. 2. (Solo reglas nuevas) Para configurar la protección de inyección de subprocesos para un proceso principal, seleccione la opción para **Seleccionar un proceso**, e introduzca el nombre del proceso en el campo facilitado. De lo contrario, deje el valor por defecto para aplicar la protección de inyección de subprocesos a **Todos los procesos**.
Paso 4	(Opcional) Defina los ajustes de inyección de subprocesos utilizando los ajustes heredados. Para utilizar los ajustes definidos por la política por defecto, habilite el módulo, y vaya a Paso 5. Alternativamente, cancele los ajustes por defecto para personalizar la configuración de inyección de subprocesos, según proceda para su organización.	1. **Habilite** o **Deshabilite** el módulo de inyección de subprocesos seleccionando la **Activación de módulos**. Solo se pueden configurar ajustes de módulos adicionales cuando el módulo está habilitado. 2. Configure la acción que se va a tomar cuando un proceso fuente intenta inyectarse en otro proceso (**Modo de proceso fuente**): • **Heredar**—Hereda la conducta de la política por defecto. • **Terminar**—Termina el proceso. • **Notificar**—Hace un log del problema y permite que el proceso se inyecte en otro proceso. 3. Configure la conducta de notificación cuando el proceso fuente intenta inyectarse en otro proceso (**Notificación de usuario**). • **Heredar**—Hereda la conducta de la política por defecto. • **On**—Informa al usuario cuando un proceso intenta inyectarse en otro proceso. • **Off**—No informa al usuario cuando un proceso intenta inyectarse en otro proceso. 4. Para añadir un proceso objetivo a una lista blanca, haga clic en el icono del modo ninja e introduzca la contraseña de supervisor. Añada uno o más procesos a la lista.

Configuración de protección de inyección de subprocesos (Continuación)		
Paso 5	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 6	(Opcional) Defina el Objetos de destino al que se aplica la regla de prevención de malware.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 7	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 8	Guarde la regla de prevención de malware.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware> Módulos de protección** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Módulos de protección.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Configuración de la protección de suspensión

La protección de suspensión protege contra una técnica de malware común en la que el atacante crea procesos en un estado suspendido, para inyectar y ejecutar el código antes de iniciarse el proceso. Cuando está habilitado, el módulo de protección de suspensión protege todos los procesos contra ataques de protección de suspensión y utiliza listas blancas para permitir que procesos legítimos comunes se inyecten en otros procesos y/o módulos.

Las reglas de políticas por defecto para la protección de suspensión suelen almacenarse en la carpeta C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Web\KnowledgeBase\Malware modules\SuspendGuard, pero puede ser diferente si se ha especificado una localización alternativa para la instalación. Puede ver los archivos de esta carpeta para determinar si existe un archivo base de política de protección de suspensión para el proceso.



Tenga cuidado a la hora de configurar nuevas reglas de protección de suspensión para evitar la cancelación de la política por defecto, lo que causará inestabilidad en el sistema operativo.

Para más información acerca de la configuración de reglas de prevención de malware, póngase en contacto con el equipo de soporte o su ingeniero de ventas.

Si el proceso no está ya protegido por la política de seguridad por defecto, puede crear una nueva regla que habilite la protección de suspensión para un proceso que utilice los ajustes de protección de suspensión por defecto o puede configurar los ajustes según sea necesario para su política de seguridad. Los ajuste incluyen el nombre del proceso, **Activación de módulos** (**Habilitar** o **Deshabilitar**), **Modo de proceso fuente** (**Terminar** o **Notificar**), **Notificación al usuario** (**On** u **Off**), y permitir módulos de función que puede invocar a procesos secundarios.

Si el proceso ya está protegido por la política de seguridad por defecto, recomendamos importar la política de protección de suspensión por defecto como nueva regla y realizar cambios para adecuarla a su organización. De este modo, cuando se activa la política, cancela la política por defecto pero sigue conteniendo los ajustes de configuración por defecto, además de los cambios realizados.

Configuración de la protección de suspensión		
Paso 1	(Opcional) Importe una copia de la política por defecto. Esto es necesario solo para procesos que ya están protegidos por la configuración por defecto y evita que se sobrescriba la política por defecto.	1. Seleccione **Políticas > Malware > Módulos de protección**. 2. En el menú , seleccione **Importar reglas**. 3. **Vaya** a los archivos de políticas por defecto de la carpeta Traps para acceder al proceso fuente deseado, y haga clic en **Cargar**. La regla importada aparece en la tabla de las reglas de prevención de malware.
Paso 2	Inicie o modifique una regla de prevención de malware.	**Añada** una nueva regla o seleccione y **Edite** una regla existente.
Paso 3	Habilite la protección de suspensión para un proceso individual o para todos los procesos.	1. Seleccione **Protección de suspensión** en la lista desplegable. 2. (Solo reglas nuevas) Para configurar la protección de suspensión para un proceso principal, seleccione la opción para **Seleccionar un proceso**, e introduzca el nombre del proceso en el campo facilitado. De lo contrario, deje el valor por defecto para aplicar la protección de suspensión a **Todos los procesos**.

Configuración de la protección de suspensión (Continuación)

Paso 4 Defina los ajustes de la protección de suspensión.

Para heredar los ajustes de la política por defecto, habilite el módulo, y vaya a Paso 5.

Alternativamente, cancele los ajustes por defecto para personalizar la configuración de protección de suspensión, según proceda para su organización.

1. **Habilite** o **Deshabilite** el módulo de protección de suspensión seleccionando la **Activación de módulos**.

   
   Solo se pueden configurar ajustes de módulos adicionales cuando el módulo está habilitado.

2. Configure la acción que se va a tomar cuando un proceso fuente intenta inyectarse en otro proceso (**Modo de proceso fuente**):
   - **Heredar**—Hereda la conducta de la política por defecto.
   - **Terminar**—Termina el proceso.
   - **Notificar**—Hace un log del problema y permite que el proceso se inyecte en otro proceso.

3. Configure la conducta de notificación cuando el proceso fuente intenta inyectarse en otro proceso (**Notificación de usuario**).
   - **Heredar**—Hereda la conducta de la política por defecto.
   - **On**—Informa al usuario cuando un proceso intenta inyectarse en otro proceso.
   - **Off**—No informa al usuario cuando un proceso intenta inyectarse en otro proceso.

4. Por defecto, la lista blanca evita que todos los módulos de función del proceso principal se inyecten en procesos secundarios. Alternativamente, se puede permitir explícitamente la inyección en las funciones y procesos secundarios añadiéndolos a una lista blanca. Para configurar los ajustes de la lista blanca, haga clic en el icono del modo ninja e introduzca la contraseña de supervisor.

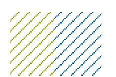
5. Herede los ajustes de lista blanca por defecto o configure procesos de función y secundarios específicos. Por defecto, la lista blanca habilita todos los módulos de función para iniciar cualquier proceso secundario. Alternativamente, puede configurar cualquiera de los siguientes y **Añadir** el nombre del módulo y el proceso secundario a la lista blanca:
   - Una función específica que inicia cualquier proceso secundario
   - Todos los nombres de función que inician un proceso secundario
   - Un nombre de función que inicia un proceso secundario

   Repita según sea necesario para añadir múltiples combinaciones por proceso principal.

Paso 5 (Opcional) Añada Condiciones a la regla.

Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.

Configuración de la protección de suspensión (Continuación)		
Paso 6	(Opcional) Defina el Objetos de destino al que se aplica la regla de prevención de malware.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 7	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 8	Guarde la regla de prevención de malware.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Malware> Módulos de protección** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Malware > Módulos de protección.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.



Administración de endpoints

Los siguientes temas describen cómo administrar los endpoints usando el Endpoint Security Manager:

- Administración de reglas de acción de Traps
- Administración de las reglas de ajustes de agentes

Administración de reglas de acción de Traps

Use *reglas de acción* para realizar acciones de una vez en el agente de Traps que se ejecuta en cada endpoint.

Reglas de acción de Traps

Las *reglas de acción* le permiten realizar acciones de una vez en el agente de Traps que se ejecuta en cada endpoint. Para cada regla de acción, debe especificarse el objeto u objetos de destino, la condición o condiciones y una de las siguientes acciones administrativas para su realización en cada endpoint:

Reglas de acción	Descripción
Gestión de archivos de datos que crea el agente de Traps	Cada endpoint almacena información de prevención y seguridad, incluidos datos históricos, volcados de memoria y archivos en cuarentena. Utilizando este tipo de acción, se pueden borrar u obtener archivos de datos que el agente de Traps crea en el endpoint. Para obtener más información, consulte Gestión de datos recopilados por Traps.
Cerrar o suspender la protección del EPM	Si una política de seguridad interfiere con una aplicación legítima, puede cerrar o suspender temporalmente la protección del Módulo de prevención de exploits (EPM) en el endpoint. Tras realizar el trabajo necesario, recomendamos analizar el evento y definir una regla de seguridad específica para esta aplicación, y volver a habilitar la protección del EPM. Para obtener más información, consulte Cerrar o suspender la protección del EPM.
Desinstalación y actualización del software Traps	Cree una regla de acción para desinstalar o actualizar Traps desde el Endpoint Security Manager. Para actualizar el software Traps en un endpoint, cargue el archivo ZIP de software en el servidor Endpoint Security Manager y especifique la ruta cuando configure la regla de acción. Para obtener más información, consulte Desinstalación o actualización de Traps en el endpoint.
Actualización o revocación de la licencia de Traps	El Endpoint Security Manager distribuye licencias al agente de Traps. Puede actualizar o revocar esa licencia en un endpoint en cualquier momento. Para obtener más información, consulte Actualización o revocación de la licencia de Traps en el endpoint.



Traps no aplica reglas de acción hasta que el agente recibe la política de seguridad actualizada, generalmente con la siguiente comunicación heartbeat con el servidor. Para obtener manualmente la política de seguridad más reciente del servidor ESM, seleccione **Actualizar ahora** en la consola de Traps.

Puede crear o editar reglas de acción en el resumen **Acciones** y la página de administración (**Ajustes > Acciones de agentes**). La selección de una regla muestra información adicional acerca de la regla y otras acciones que se pueden tomar (**Duplicar**, **Borrar**, o **Activar**/**Desactivar** la regla). Para obtener más información, consulte Administración de reglas de acción de Traps.

Añadir una nueva regla de acción

Para cada regla de acción, puede especificarse el objeto u objetos de la organización, la condición o condiciones y la acción o acciones para su realización en cada endpoint.

Añadir una nueva regla de acción		
Paso 1	Inicie una nueva regla de acción.	Seleccione **Ajustes > Acciones de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Seleccione el tipo de tarea que desea realizar.	Seleccione uno de los siguientes de la lista desplegable **Tareas**, y configure los ajustes según el tipo de acción: • **Datos de agentes**— Para más información, consulte Gestión de datos recopilados por Traps. • **Servicio de agentes**— Para más información, consulte Cerrar o suspender la protección del EPM. • **Instalación de agentes**— Para más información, consulte Desinstalación o actualización de Traps en el endpoint. • **Licencia de agentes**— Para más información, consulte Actualización o revocación de la licencia de Traps en el endpoint.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de acción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de acción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Acciones de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Acciones de agentes**. Desde ahí, puede **Duplicar**, **Borrar**, o **Desactivar** la regla, según sea necesario.

Gestión de datos recopilados por Traps

Utilice el asistente de acción para realizar las siguientes acciones para los archivos de datos que Traps crea en el endpoint:

Acción	Descripción
Borrar historial	Cada endpoint guarda un historial de las prevenciones de seguridad. Seleccione esta opción para borrar los archivos de datos históricos y que no se visualicen en la consola de Traps.
Borrar volcados de memoria	Los volcados de memoria son registros de los contenidos de la memoria del sistema cuando se produce un evento de prevención. Seleccione esta opción para borrar los registros de la memoria del sistema en los objetos de destino.
Borrar archivos en cuarentena	Cuando se produce un evento de seguridad en un endpoint, Traps captura volcados de memoria y archivos recientes asociados con el evento y los almacena en la carpeta forense del endpoint. Seleccione esta opción para borrar los archivos asociados con el evento de seguridad de los objetos de destino.
Obtención de datos que recopila el agente	Traps recopila el historial de eventos de seguridad, volcados de memoria y otras informaciones asociadas con un evento de seguridad. Seleccione esta opción para recopilar toda la información guardada de todos los eventos ocurridos en el endpoint. Tras ejecutar esta regla, los agentes de Traps envían todos los datos relacionados con la prevención, incluido un volcado de memoria del proceso protegido, a la carpeta forense designada.
Obtención de logs que recopila el agente	Traps recopila logs detallados de rastros de las aplicaciones y guarda información acerca de los procesos y aplicaciones que se ejecutan en el endpoint. Utilice el archivo de logs para depurar un problema con una aplicación o investigar un problema específico que se ha escrito en el log. La selección de esta opción crea una regla de acción para recopilar toda la información de restos de aplicación para un endpoint. Tras ejecutarse esta regla, el agente de Traps envía todos los logs a la carpeta forense.

Gestión de los datos que obtiene Traps		
Paso 1	Inicie una nueva regla de acción.	Seleccione **Ajustes > Acciones de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Defina las tareas que se van a realizar en los datos de Traps guardados en los endpoints.	1. Seleccione **Datos de agentes** en la lista desplegable **Tareas**. 2. Seleccione una o más de las opciones para la administración de los datos de agentes. • Borrar historial • Borrar volcados de memoria • Borrar archivos en cuarentena • Obtener datos recopilados de los agentes • Obtener logs recopilados de los agentes
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.

Gestión de los datos que obtiene Traps (Continuación)		
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de acción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de acción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Acciones de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Acciones de agentes**. Desde ahí, puede **Duplicar**, **Borrar**, o **Desactivar** la regla, según sea necesario.

Cerrar o suspender la protección del EPM

Si una política de seguridad interfiere con una aplicación legítima, puede cerrar o suspender temporalmente la inyección del Módulo de prevención de exploits (EPM) en un endpoint. Para los endpoints que ejecutan Traps versión 3.1 o posterior, Traps no inyectar los EPM en los procesos mientras la regla esté activa, pero enviará notificaciones acerca de eventos de seguridad.

Tras realizar el trabajo necesario, recomendamos analizar el evento y definir una regla de seguridad específica para esta aplicación, y habilitar la protección del EPM. En el caso de la suspensión del EPM, la regla habilita automáticamente la protección de EPM después de transcurrir la duración especificada. En el caso de cierre del EPM, debe reiniciarse manualmente el endpoint para iniciar el servicio de Traps en el endpoint y volver a habilitar la protección del EPM.

Cerrar o suspender la protección del EPM		
Paso 1	Inicie una nueva regla de acción.	Seleccione **Ajustes > Acciones de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Defina la duración para la protección de suspensión.	1. Seleccione **Servicio de agentes** en la lista desplegable **Tareas**. 2. Seleccione **Protección de suspensión para** y especifique la duración en minutos en la lista desplegable, **10**, **30**, **60**, o **180 minutos**—para suspender temporalmente la inyección de módulos de seguridad.

Cerrar o suspender la protección del EPM (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de acción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de acción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Acciones de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Acciones de agentes**. Desde ahí, puede **Duplicar**, **Borrar**, o **Desactivar** la regla, según sea necesario.

Desinstalación o actualización de Traps en el endpoint

Cree una nueva regla de acciones de agente para desinstalar Traps de objetos de destino o actualizar Traps usando el software accesible desde la consola ESM.

Desinstalación o actualización de Traps en el endpoint		
Paso 1	Inicie una nueva regla de acción.	Seleccione **Ajustes > Acciones de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Defina las tareas que se van a realizar en Traps en los endpoints.	Seleccione **Instalación de agentes** en la lista desplegable **Tareas** y seleccione una de las siguientes acciones: • **Desinstalar** • **Actualizar desde la ruta**—Vaya al archivo ZIP de instalación y haga clic en **Cargar**.

Desinstalación o actualización de Traps en el endpoint (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de acción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de acción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Acciones de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Acciones de agentes**. Desde ahí, puede **Duplicar**, **Borrar**, o **Desactivar** la regla, según sea necesario.

Actualización o revocación de la licencia de Traps en el endpoint

Cree una nueva regla de acción para actualizar o revocar una licencia del servicio Traps bajo ejecución en un endpoint. La revocación de una licencia le permite reasignar una licencia a otro endpoint. Tras revocar una licencia, Traps no protegerá el endpoint. Utilice la opción de actualización para sustituir una licencia en el endpoint y reanudar el servicio de Traps.

Actualización o revocación de la licencia de Traps en el endpoint		
Paso 1	Inicie una nueva regla de acción.	Seleccione **Ajustes > Acciones de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Defina las tareas que se van a realizar en la licencia de Traps en los endpoints.	Seleccione **Licencia de agentes** en la lista desplegable **Tareas** y seleccione una de las siguientes acciones: • **Actualizar**—Actualiza la licencia de Traps en un endpoint. • **Revocar**—Revoca una licencia y detiene el servicio del agente en un endpoint.

Actualización o revocación de la licencia de Traps en el endpoint (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de acción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de acción.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Acciones de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Acciones de agentes**. Desde ahí, puede **Duplicar**, **Borrar**, o **Desactivar** la regla, según sea necesario.

Administración de las reglas de ajustes de agentes

Use las *reglas de ajustes de agentes* para cambiar las preferencias relacionadas con Traps desde una localización central.

Reglas de ajustes de agentes de Traps

Las *reglas de ajustes de agentes* le permiten cambiar las preferencias relacionadas con Traps desde una localización central. En la página **Ajustes > Ajustes de agentes** puede crear reglas para administrar los siguientes ajustes de Traps:

Reglas de ajustes de agentes	Descripción
Ajustes de logs de eventos	Determinan la forma en que el agente de Traps administra los logs de eventos. Incluye la selección de un tamaño para los logs de endpoints y, opcionalmente, el envío de los logs de endpoints al log de eventos de Windows. Para obtener más información, consulte Definición de las preferencias de logging de eventos.
Ajustes de visibilidad de usuario y acceso	Determinan si el usuario final puede acceder a la aplicación de la consola de Traps y qué manera. Opcionalmente, se puede configurar la consola de modo que solo sea accesible para los administradores. Para obtener más información, consulte Ocultación o restricción de acceso a la consola de Traps.
Ajustes de heartbeat	Determinan la frecuencia con la que el agente de Traps envía el mensaje heartbeat al servidor ESM. La frecuencia óptima se determina según el número de endpoints de la organización y la carga típica de red. El periodo heartbeat por defecto es de cinco minutos. Para obtener más información, consulte Definición de ajustes de comunicación entre el endpoint y el servidor ESM.
Recopilación de información de nuevos procesos	Configure los agentes Traps para recopilar nuevos procesos de los endpoints. Cuando esta opción está habilitada, Traps informa al servidor ESM de cada proceso que se ejecuta en un endpoint. Puede ver los procesos en la vista de Administración de procesos de las pantallas del Endpoint Security Manager y decidir si desea crear reglas de seguridad relacionadas con los procesos. Para obtener más información, consulte Recopilación de información de nuevos procesos.

Reglas de ajustes de agentes	Descripción
Protección de servicio	Evita los intentos de deshabilitar o hacer cambios en los valores de registro y campos de Traps. Cuando esta opción está habilitada, los usuarios no pueden cerrar o modificar el servicio del agente de Traps. Para obtener más información, consulte Gestión de protección de servicios.
Seguridad de agentes	Por defecto, los usuarios y administradores debe introducir la contraseña necesaria para desinstalar la aplicación Traps. Utilice esta opción para cambiar la contraseña. Para obtener más información, consulte Cambio de la contraseña de desinstalación.
Mensaje de prevención	Personalice el título, pie e imagen de pantalla para los mensajes emergentes de prevención que Traps muestra cuando se produce un evento de seguridad en el endpoint. Para obtener más información, consulte Creación de un mensaje de prevención personalizado.
Mensaje de notificación	Personalice el título, pie e imagen de pantalla para los mensajes emergentes de notificación que Traps muestra cuando se activa una conducta de notificación en el endpoint. Para obtener más información, consulte Creación de un mensaje de prevención personalizado.



Traps no aplica reglas de ajustes de agentes hasta que el agente de Traps recibe la política de seguridad actualizada, generalmente con la siguiente comunicación heartbeat con el servidor. Para obtener manualmente la política de seguridad más reciente del servidor ESM, seleccione **Actualizar ahora** en la consola de Traps.

Puede crear o editar ajustes de agentes en el resumen Acjustes de agentes y la página de administración (**Ajustes > Ajustes de agentes**). La selección de una regla muestra información adicional acerca de la regla y otras acciones que se pueden tomar (**Borrar**, **Activar**/**Desactivar**, o **Editar** la regla). Para obtener más información, consulte Administración de las reglas de ajustes de agentes.

Añadir una nueva regla de ajustes de agentes

Para cada regla de ajustes de agentes, puede especificar el objeto y objetos de la organización, la condición o condiciones y las preferencias de Traps que desea aplicar.

Añadir una nueva regla de ajustes de agentes		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.

Añadir una nueva regla de ajustes de agentes (Continuación)		
Paso 2	Seleccione el tipo de ajuste que desea cambiar y configure sus preferencias.	Seleccione uno de los siguientes y configure los ajustes según el tipo de preferencia: • **Logging de eventos**—Para más información, consulte Definición de las preferencias de logging de eventos. • **Visibilidad y acceso de usuario**—Para más información, consulte Ocultación o restricción de acceso a la consola de Traps. • **Ajustes de heartbeat**—Para más información, consulte Definición de ajustes de comunicación entre el endpoint y el servidor ESM. • **Administración de procesos**—Para más información, consulte Recopilación de información de nuevos procesos. • **Protección de servicio**—Para más información, consulte Gestión de protección de servicios. • **Seguridad de agentes**—Para más información, consulte Cambio de la contraseña de desinstalación. • **Mensaje de prevención**—Para más información, consulte Creación de un mensaje de prevención personalizado. • **Mensaje de notificación**—Para más información, consulte Creación de un mensaje de prevención personalizado.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes**. Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

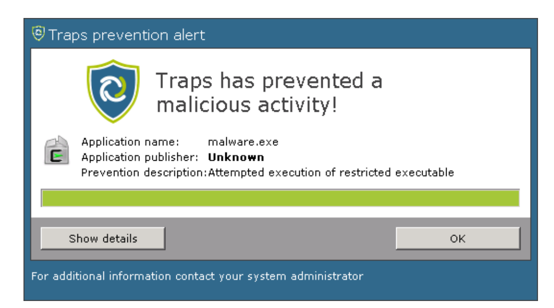
Definición de las preferencias de logging de eventos

El log de eventos de Windows guarda eventos de aplicaciones, seguridad y el sistema que pueden ayudarle a diagnosticar la fuente de problemas del sistema. Utilice el asistente de ajustes de agentes para especificar si enviar o no eventos de seguridad encontrados por Traps al log de eventos de Windows para definir un rango de tamaño para la carpeta de almacenamiento local temporal que Traps utiliza para almacenar información de eventos.

Definición de las preferencias de logging de eventos		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Defina los ajustes de logging de eventos para los endpoints.	1. Seleccione **Logging de eventos** en la lista desplegable **Ajustes de agentes**. 2. Realice una o más de las siguientes acciones: • Seleccione la opción **Ajustar tamaño de disco (MB)** para especificar el tamaño de la carpeta de almacenamiento temporal que utilizará Traps para almacenar logs de eventos. Especifique el tamaño máximo en MB. El valor predeterminado es de 1000 MB (10 GB). El máximo es de 10.000.000 MB (10 TB). • Seleccione la opción **Escribir eventos de agentes en el log de eventos de Windows** para enviar los eventos de Traps al log de eventos de Windows.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes**. Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Ocultación o restricción de acceso a la consola de Traps

Por defecto, un usuario puede acceder a la consola de Traps para ver información relacionada con el estado actual del endpoint, eventos de seguridad y cambios en la política de seguridad. Cuando se activa un evento de seguridad, el usuario también recibe una notificación acerca del evento incluidos el nombre de la aplicación, el editor, y una descripción de la regla de prevención o restricción que ha activado la notificación.



Puede crear una regla de ajustes de agentes para cambia la accesibilidad de la consola y especificar si se ocultan o no notificaciones del usuario.

Ocultación o restricción de acceso a la consola de Traps		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Defina la visibilidad del usuario y los ajustes de acceso para los endpoints.	1. Seleccione **Disponiblidad y acceso de usuario** en la lista desplegable **Ajustes de agentes**. 2. Seleccione una o más de las siguientes opciones: • **Ocultar icono de bandeja**—La instalación de Traps en un endpoint añade un icono al área de notificación (bandeja del sistema) por defecto. Utilice esta opción para ocultar el icono de bandeja del endpoint. • **Desactivar el acceso a la consola de Traps**—Por defecto, el usuario puede acceder a la consola de Traps activándola desde la bandeja del sistema. Utilice esta opción para deshabilitar la capacidad de activación de la consola. • **Ocultar notificación de usuario de Traps**—Cuando el agente de Traps encuentra un evento de prevención, el usuario ve un mensaje de notificación que describe el evento. Utilice esta opción para ocultar notificaciones.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.

Ocultación o restricción de acceso a la consola de Traps (Continuación)		
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Definición de ajustes de comunicación entre el endpoint y el servidor ESM

Con regularidad, el endpoint se comunica con el Endpoint Security Manager enviando mensajes heartbeat e informa al servidor ESM. Durante la comunicación heartbeat, el agente de Traps solicita la política de seguridad actual y envía una respuesta al Endpoint Security Manager para informar del estado del endpoint. Se denomina ciclo heartbeat la frecuencia con la que el agente de Traps envía mensajes heartbeat al servidor ESM. La frecuencia óptima se determina según el número de endpoints de la organización y la carga típica de red. El periodo heartbeat por defecto es de cinco minutos.

El agente de Traps también envía cambios de informes en el servicio incluidos inicios, paradas y eventos de bloqueo y los procesos descubiertos en el endpoint. Se denomina intervalo de informes a la frecuencia con la que el agente de Traps envía notificaciones de informes.

Definición de ajustes de comunicación entre el endpoint y el servidor ESM		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Defina los ajustes heartbeat para los endpoints.	1. Seleccione **Ajustes de heartbeat** en la lista desplegable **Ajustes de agentes**. 2. Seleccione una o más de las siguientes opciones: • **Ajuste definido del ciclo heartbeat**—Especifique la frecuencia en **Horas**, **Minutos**, o **Días**. • **Ajuste de intervalo de envío de informes**—Especifique la frecuencia en **Horas**, **Minutos**, o **Días**.

Definición de ajustes de comunicación entre el endpoint y el servidor ESM (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Recopilación de información de nuevos procesos

Con la recopilación de información procesos nuevos del endpoint, puede analizar si se crearán o no reglas de seguridad. Por defecto, el agente de Traps no recopila información sobre procesos nuevos. Puede configurar Traps para informar de cada proceso ejecutado en un endpoint al Endpoint Security Manager habilitando el ajuste **Administración de procesos**. La página de administración de procesos muestra todos los procesos añadidos manualmente o descubiertos automáticamente.

Recopilación de información de nuevos procesos		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Habilite la recopilación de nuevos procesos en los endpoints.	1. Seleccione **Administración de procesos** en la lista desplegable **Ajustes de agentes**. 2. Seleccione la casilla de verificación **Recopilar información de nuevos procesos**. Según se detectan nuevos procesos, el ESM los muestra en la página **Políticas > Exploit > Administración de procesos** como procesos desprotegidos. Defina reglas para proteger los nuevos procesos, según sea necesario.

Recopilación de información de nuevos procesos (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes**. Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Gestión de protección de servicios

La protección de servicios le permite proteger la ejecución de servicios de Traps en sus endpoint.s. Cuando se habilita la protección de servicios, los usuarios no pueden cambar los valores de registro o archivos asociados con Traps, o parar o modificar el servicio de Traps, de un modo u otro.

Gestión de protección de servicios		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Habilite la protección de servicios.	1. Seleccione **Protección de servicios** en la lista desplegable **Ajustes de agentes**. 2. Seleccione **Habilitar protección de servicios** o **Deshabilitar protección de servicios**.

Gestión de protección de servicios (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

Cambio de la contraseña de desinstalación

Por defecto, debe introducir la contraseña de desinstalación especificada durante la instalación para desinstalar Traps de un endpoint. Cambie la contraseña por defecto creando una regla de ajustes de agentes.

Cambio de la contraseña de desinstalación		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Cambie la contraseña	1. Seleccione **Seguridad de agentes** en la lista desplegable. Seleccione la casilla **Definir contraseña de desinstalación**. 2. Introduzca la contraseña que el usuario o administrador deben introducir para desinstalar Traps. La contraseña debe tener una longitud mínima de ocho caracteres.

Cambio de la contraseña de desinstalación (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

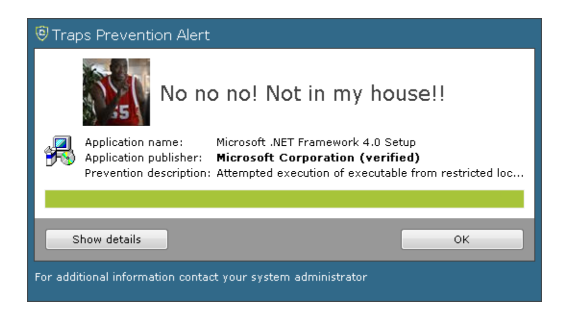
Creación de un mensaje de prevención personalizado

Traps muestra mensajes de prevención cuando un archivo o proceso violan una política de seguridad y la conducta de terminación se configura para bloquear el archivo e informar al usuario. Utilice una regla de ajustes de agentes para personalizar el título, pie e imagen de pantalla para los mensajes emergentes de prevención que Traps muestra cuando se produce un evento de seguridad en el endpoint.

Creación de un mensaje de prevención personalizado		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.

Creación de un mensaje de prevención personalizado (Continuación)	
Paso 2 Personalice una o más opciones de mensajes de prevención.	1. Seleccione **Mensaje de prevención** en la lista desplegable. 2. Según realiza los cambios, la vista previa a la derecha de los ajustes de configuración muestra los cambios. • **Título de prevención**—Introduzca un máximo de 50 caracteres en el campo facilitado para mostrar un título de notificación personalizado. • **Acción de prevención**—Para facilitar información de contacto o de otro tipo en la parte inferior del mensaje, introduzca hasta 250 caracteres en el campo de acción de notificación. Para especificar una dirección de correo electrónico, utilice el formato HTML estándar, por ejemplo `<a href="mailto://support@your_organization.com"> Help Desk</a>`. • **Imagen de prevención**—Para sustituir el logotipo de Traps por una nueva imagen, **Vaya** a una nueva imagen, y haga clic en **Cargar**.
Paso 3 (Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4 (Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5 (Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6 Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes.** Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.

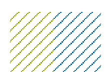
Creación de un mensaje de prevención personalizado



Traps muestra imágenes de notificación cuando la conducta de notificación se configura para alertar al usuario. Utilice una regla de ajustes de agentes para personalizar el título, pie e imagen de pantalla para el mensaje emergente de prevención que Traps muestra cuando se produce la conducta activa una notificación de alerta.

Creación de un mensaje de notificación personalizado		
Paso 1	Inicie una nueva regla de ajustes de agentes.	Seleccione **Ajustes > Ajustes de agentes** y, a continuación, **Añadir** una nueva regla.
Paso 2	Personalice una o más opciones de mensajes de notificación.	1. Seleccione **Mensaje de notificación** en la lista desplegable. 2. Según realiza los cambios, la vista previa a la derecha de los ajustes de configuración muestra los cambios. • **Título de notificación**—Introduzca un máximo de 50 caracteres en el campo facilitado para mostrar un título de notificación personalizado. • **Acción de notificación**—Para facilitar información de contacto o de otro tipo en la parte inferior del mensaje, introduzca hasta 250 caracteres en el campo de acción de notificación. Para especificar una dirección de correo electrónico, utilice el formato HTML estándar, por ejemplo `<a href="mailto://support@your_organization.com"> Help Desk</a>`. • **Imagen de notificación**—Para sustituir el logotipo de Traps por una nueva imagen, **Vaya** a una nueva imagen, y haga clic en **Cargar**.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.

Creación de un mensaje de notificación personalizado (Continuación)		
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de ajustes de agentes.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre** y borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla de ajustes de agentes.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Ajustes > Ajustes de agentes** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Ajustes > Ajustes de agentes**. Desde ahí, puede **Borrar** o **Desactivar** la regla, según sea necesario.



Datos forenses

Descripción general de datos forenses

Flujo de datos forenses



Fase 1: Activación de eventos de prevención

Cuando se produce un intento de ataque sobre una vulnerabilidad de software, los módulos de protección de Traps entran en acción para detener la conducta de proceso malintencionado y, finalmente, bloquear el ataque. Por ejemplo, considere el caso en el que un archivo intenta acceder a metadatos de DLL cruciales desde localizaciones de códigos que no son de confianza. Si se activa el módulo de seguridad de DLL para proteger procesos de su organización, Traps detiene inmediatamente el proceso que intenta acceder a los metadatos de DLL. Traps registra el evento en su log de eventos e informa al usuario del evento de seguridad. Se así se ha configurado, Traps muestra un mensaje de notificación personalizado (para más información, consulte Creación de un mensaje de prevención personalizado).

Tras detener con éxito un intento de exploit, Traps recoge y analiza los datos relacionados con el evento según se describe en Fase 2: Análisis automatizado.

Fase 2: Análisis automatizado

Cuando se produce un evento de seguridad en un endpoint, Traps congela los contenidos de la memoria, y los guarda en un archivo conocido como volcado de memoria. Desde la consola ESM se puede ajustar la configuración del volcado de memoria que especifica su tamaño como pequeño, mediano o completo (el conjunto de información más grande y más completo), y Traps cargará automáticamente el volcado de memoria en la carpeta forense. Para obtener más información, consulte Definición de las preferencias del volcado de memoria.

Tras crear un volcado de memoria, Traps decodifica el archivo y extrae la información para identificar la causa subyacente y verificar la validez de la prevención. Utilice los resultados del análisis para diagnosticar y comprender el evento.

Dependiendo del tipo de evento, Traps también puede usar herramientas de detección automatizadas para explorar la conducta malintencionada, según se describe en Fase 3: Detección automatizada.

Fase 3: Detección automatizada

Tras analizar el volcado de memoria, Traps realiza automáticamente un análisis secundario, cuyos resultados se pueden usar para verificar la legitimidad de un evento de prevención. El análisis secundario proporciona una visión más amplia de la naturaleza del evento usando las herramientas de detección, incluida la detección de la cadena ROP y la detección de heap spray, para identificar rastros de actividades malintencionadas adicionales.

Si las herramientas de detección identifican con éxito los restos de actividades malintencionadas, Traps guarda la información en un archivo de log del sistema en el endpoint, usando la sintaxis siguiente: Prefijo único de Traps client ID-event ID. Traps también informa de la detección al servidor ESM. La consola ESM muestra los resultados en la sección **Análisis de vuelco automático de Traps** para cada registro de eventos de prevención, incluido si cada herramienta de detección ha identificado con éxito actividad malintencionada adicional. Si Traps no captura la memoria, crea el archivo de vuelco incorrectamente o no logra completar el análisis secundario, la consola ESM oculta esta sección en el registro de eventos.

Si las herramientas de detección identifican uno o más rastros de actividad maliciosa, existe una alta probabilidad de que el evento de prevención sea una amenaza legítima.

Para la posterior solución de problemas o análisis de eventos de seguridad, observe los datos forenses que Traps recopila según se describe en Fase 4: Recopilación de datos forenses.

Fase 4: Recopilación de datos forenses

Tras analizar los archivos, Traps informa al ESM del evento de seguridad y puede enviar datos forenses adicionales a la carpeta forense.

Si su política de seguridad contiene un regla de recopilación de datos forenses, Traps recopila uno o más tipos de datos especificados y carga el archivo o archivos en la carpeta forense. Dependiendo de las preferencias, Traps puede recopilar URI a los que se ha accedido, controladores, archivos y DLL relevantes que se cargan en la memoria bajo procesos atacados, y procesos antecesores del proceso que activaron el evento de seguridad. Para obtener más información, consulte Definición de las preferencias de recopilaciones forenses.

Por defecto, Traps utiliza una carpeta de Servicio de transferencia inteligente en segundo plano (BITS) basada en la web que utiliza ancho de banda de red inactiva para cargar los datos. Para obtener más información, consulte Cambio de la carpeta forense por defecto.

También puede obtener manualmente datos forenses para un evento de seguridad específico creando una regla de acción de una vez para obtener los datos. Para obtener más información, consulte Obtención de datos acerca de un evento de seguridad. Para ver el estado de la carga forense, seleccione **Monitor > Obtención de informes forenses**.

Tipos de datos forenses

Cuando se produce un evento de seguridad en un endpoint, Traps puede recopilar la información siguiente:

Tipo de datos forenses	Descripción
Volcado de memoria	Contenidos de localizaciones de memoria capturados cuando se produce un evento.
Archivos accedidos	Archivos que se cargan en la memoria bajo el proceso atacado para la inspección detallada del evento, incluidos: • Logs detallados de rastros de aplicación • Obtención de DLL relevantes, incluida su ruta • Archivos relevantes de la carpeta de archivos temporales de Internet. • Archivos abiertos (ejecutables y no ejecutables)
Módulos cargados	Controladores que se cargan en el sistema en el momento de un evento de seguridad.
URI accedido	Un identificador de recursos uniformes (URI) habilita la interacción con el recurso y ayuda a identificarlo. Recursos de red a los que se ha accedido en el momento del evento de seguridad y la información del URI, incluidos: • Los URI de todos los navegadores principales, incluidos enlaces ocultos y tramas de los hilos atacados relevantes • URI fuente de applets de Java, nombres y rutas de archivos, incluidos procesos padre, abuelo y hijo. • La recopilación de llamadas de URI de plug-ins del navegador, reproductores multimedia y software de clientes de correo
Procesos antecesores	Información sobre procesos antecesores, de navegadores, no navegadores y procesos hijo de applets de Java, en el momento de un evento de seguridad, incluidos: • Fuentes y destinos separados para inyección de subprocesos • Procesos hijo, padre y abuelo restringidos

Administración de reglas y ajustes forenses

Reglas forenses

Las *reglas forenses* le permiten obtener datos forenses capturados por Traps desde una localización central. En la página **Políticas > Informes forenses**, puede crear reglas para administrar los siguientes ajustes forenses:

Reglas de ajustes de agentes	Descripción
Ajustes de volcado de memoria	Especifique los ajustes de volcado, incluido el tamaño para el volcado de memoria y habilite Traps para el envío automático del volcado de memoria al servidor. Esta configuración solo se aplica a los datos recopilados de los eventos de prevención relacionados con los procesos protegidos. Para obtener más información, consulte Definición de las preferencias del volcado de memoria.
Recopilación forense	Habilite Traps para la recopilación de datos forenses de cada evento de seguridad, incluidos los archivos a los que se ha accedido, los módulos cargados en la memoria, los URI a los que se ha accedido y los procesos antecesores del proceso que han activado el evento de seguridad. Para obtener más información, consulte Definición de las preferencias de recopilaciones forenses.

Cambio de la carpeta forense por defecto

Cambio del destino de la carpeta forense utilizando la consola ESM

Para una solución adicional de problemas o el análisis de eventos de seguridad, como una prevención o bloqueo, Traps carga los datos forenses en una carpeta forense basada en la web. Durante la instalación de la consola ESM, el instalador habilita el Servicio de transferencia inteligente en segundo plano (BITS) que utiliza ancho de banda de red inactiva para cargar los datos en la carpeta forense.

Para analizar un evento de seguridad, cree una regla de acción para obtener los datos forenses del endpoint (consulte Gestión de datos recopilados por Traps). Cuando Traps recibe la solicitud de envío de datos, copia los archivos en la carpeta forense (también denominada en el Endpoint Security Manager carpeta de cuarentena), que es una ruta local o de red que se especifica durante la instalación inicial.

Puede cambiar la ruta de la carpeta forense en cualquier momento usando el Endpoint Security Manager o la herramienta de configuración DB (consulte Cambio del destino de la carpeta forense utilizando la herramienta de configuración DB). Todos los endpoints deben tener permiso de escritura para esta carpeta.

Cambio del destino de la carpeta forense utilizando la consola ESM	
Paso 1	Seleccione **Configuración > General** y, a continuación, seleccione **Configuración del servidor** de la lista desplegable.
Paso 2	Introduzca la URL basada en la web en el campo **URL de carpeta forense** con el fin de utilizar BITS para cargar los datos forenses. Por ejemplo, **http://ESMserver:80/BitsUploads**.  Si utiliza SSL, incluya el nombre de dominio totalmente cualificado (FQDN) en la ruta, por ejemplo, **https://ESMserver.Domain.local:443/BitsUploads**.

Cambio del destino de la carpeta forense utilizando la herramienta de configuración DB

Para una solución adicional de problemas o el análisis de eventos de seguridad, como una prevención o bloqueo, Traps carga los datos forenses en una carpeta forense basada en la web. Durante la instalación de la consola ESM, el instalador habilita el Servicio de transferencia inteligente en segundo plano (BITS) que utiliza ancho de banda de red inactiva para cargar los datos en la carpeta forense.

Para analizar un evento de seguridad, cree una regla de acción para obtener los datos forenses del endpoint (consulte Gestión de datos recopilados por Traps). Cuando Traps recibe la solicitud de envío de datos, copia los archivos en la carpeta forense (también denominada en el Endpoint Security Manager carpeta de cuarentena), que es una ruta local o de red que se especifica durante la instalación inicial.

Puede cambiar la ruta de la carpeta forense en cualquier momento usando el Endpoint Security Manager (consulte Cambio del destino de la carpeta forense utilizando la consola ESM) o usando la herramienta de configuración de bases de datos (DB).

La herramienta de configuración DB es una interfaz de línea de comandos que proporciona una alternativa a la gestión de los ajustes básicos del servidor utilizando la consola EMS. Puede acceder a la herramienta de configuración DB utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. La herramienta de configuración DB se encuentra en la carpeta Servidor del servidor ESM.



Todos los comandos ejecutados utilizando la herramienta de configuración DB hacen distinción entre mayúsculas y minúsculas.

Cambio del destino de la carpeta forense utilizando la herramienta de configuración DB	
Paso 1	Abra una línea de comando como administrador: • Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**. • Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL**+**Mayús.**+**INTRO**.
Paso 2	Vaya a la carpeta que contiene la herramienta de configuración DB: `C:\Users\Administrator>cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server`

Cambio del destino de la carpeta forense utilizando la herramienta de configuración DB	

Paso 3	(Opcional) Visualice los ajustes de servidor existentes:
	`C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig server show`**
	`PreventionsDestFolder = \\ESMServer\Quarantine`
	`InventoryInterval = 284`
	`HeartBeatGracePeriod = 4200`
	`NinjaModePassword = Password2`
	`BitsUrl = https://CYVERASERVER.Domain.local:443/BitsUploads`
	`MaxActions = 5000`

Paso 4	Introduzca la URL basada en la web de la carpeta forense. `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig server BitsUrl http://ESMserver:80/BitsUploads`**  Si utiliza SSL, incluya el nombre de dominio totalmente cualificado (FQDN) en la ruta, por ejemplo, **https://ESMserver.Domain.local:443/BitsUploads**.

Paso 5	(Opcional) Para verificar la ruta de la carpeta forense, ejecute el comando `dbconfig server show`:
	`C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig server show`**
	`PreventionsDestFolder = \\ESMServer-New\Quarantine`
	`InventoryInterval = 284`
	`HeartBeatGracePeriod = 4200`
	`NinjaModePassword = Password2`
	`BitsUrl = HTTPS://ESMserver.Domain.local:443/BitsUploads`
	`MaxActions = 5000`

Creación de una regla forense

Cree una regla forense para definir el volcado de memoria y las preferencias de recopilaciones forenses.

Creación de una regla forense		
Paso 1	Inicie una nueva regla forense.	Seleccione **Políticas > Datos forenses** y, a continuación, haga clic en **Añadir**.
Paso 2	Seleccione el tipo de regla que desea configurar.	Seleccione uno de los siguientes de la lista desplegable **Datos forenses**, y configure los ajustes según el tipo de regla: • **Volcado de memoria**—Para más información, consulte Definición de las preferencias del volcado de memoria. • **Recopilación de datos forenses**—Para más información, consulte Definición de las preferencias de recopilaciones forenses.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.

Creación de una regla forense (Continuación)		
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla forense.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Datos forenses** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Datos forenses**. Desde ahí, puede **Activar** o **Desactivar** la regla, según sea necesario.

Definición de las preferencias del volcado de memoria

Cuando un proceso protegido se ha bloqueado o ha terminado de forma anómala, Traps registra información acerca del evento, incluidos los contenidos de las localizaciones de memoria y otros datos acerca del evento, en lo que se conoce como volcado de memoria.

Cree una regla forense para determinar el modo en que Traps administra volcados de memoria relacionados con el proceso, incluido si se envían volcados de memoria automáticamente a la carpeta forense o si se cambia el tamaño del volcado de memoria, pequeño, mediano o completo (el conjunto de información más grande y más completo).

Definición de las preferencias del volcado de memoria		
Paso 1	Inicie una nueva regla forense.	Seleccione **Políticas > Datos forenses** y, a continuación, haga clic en **Añadir**.
Paso 2	Defina las preferencias del volcado de memoria cuando se produzca un evento de prevención en el endpoint.	1. Seleccione **Volcado de memoria** en la lista desplegable **Datos forenses** y seleccione una de las siguientes preferencias: • Envíe automáticamente los volcados de memoria al servidor seleccionando **Enviar los volcados de memoria automáticamente**. • Especifique el tamaño del volcado de memoria seleccionando la opción **Tamaño de volcado de memoria** y, a continuación, seleccionando **Pequeño**, **Mediano**, o **Completo** en la lista desplegable. 2. Seleccione una o más aplicaciones. Traps aplicará el ajuste a las aplicaciones seleccionadas.

Definición de las preferencias del volcado de memoria (Continuación)		
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla forense.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Datos forenses** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Datos forenses.** Desde ahí, puede **Activar** o **Desactivar** la regla, según sea necesario.

Definición de las preferencias de recopilaciones forenses

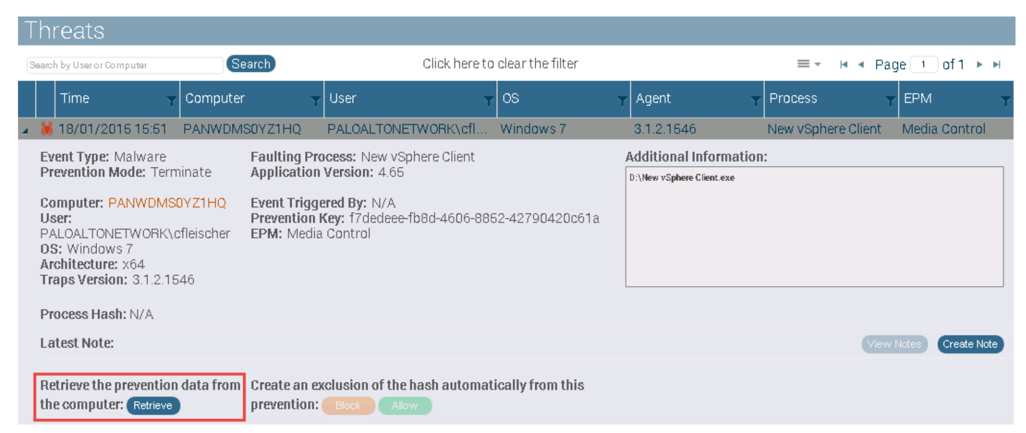
Para ayudarle a entender mejor y derivar implicaciones acerca de la verdadera naturaleza de un evento de seguridad cuando se produce en un endpoint, puede configurar las opciones de recopilaciones forenses. Cuando se produzca un evento de seguridad, Traps puede hacer un informe de los archivos a los que se ha accedido, los módulos que se han cargado en la memoria, los URI a los que se ha accedido y los procesos antecesores del proceso que han activado el evento de seguridad.

Definición de las preferencias de recopilaciones forenses		
Paso 1	Inicie una nueva regla forense.	Seleccione **Políticas > Datos forenses** y, a continuación, haga clic en **Añadir**.

Definición de las preferencias de recopilaciones forenses (Continuación)		
Paso 2	Defina las preferencias de recopilaciones forenses.	Seleccione **Recopilación de datos forenses** de la lista desplegable **Datos forenses** y configure las preferencias en los campos siguientes: • **Informar de archivos accedidos**—Seleccione **Habilitado** para recopilar información acerca de los archivos relacionados con un evento de seguridad y las DLL relevantes que se cargan en la memoria bajo el proceso atacado para una inspección en profundidad de los eventos. • **Informar de módulos cargados**—Seleccione **Habilitado** para informar de los controladores cargados en el sistema en el momento de la aparición de un evento de seguridad. • **Informar de URI accedido**—Seleccione **Habilitado** para recopilar información de los URI de los plug-ins de la web, reproductores multimedia y clientes de correo. • **Informar de procesos antecesores**—Algunas aplicaciones pueden ejecutar applets de Java como proceso hijo, e incluso como proceso hijo de un proceso hijo, etc. Seleccione **Habilitado** para registrar información acerca de los procesos antecesores de navegadores, no navegadores, y procesos hijo de applets de Java para permitirle una mejor comprensión de la raíz de un evento. Alternativamente, para cada tipo de datos, puede deshabilitar o heredar los ajustes de la política de seguridad por defecto.
Paso 3	(Opcional) Añada Condiciones a la regla.	Por defecto, el ESM no aplica condiciones a una regla. Para especificar una condición, seleccione la pestaña **Condiciones**. A continuación, seleccione la condición en la lista Condiciones y haga clic en **Añadir**. La condición se añade a la lista Condiciones seleccionadas. Repita el procedimiento para añadir más condiciones, si así lo desea. Para añadir una condición a la lista Condiciones, consulte Definición de condiciones de activación para una regla.
Paso 4	(Opcional) Defina el Objetos de destino al que se aplica la regla de restricción.	Por defecto, el ESM aplica las nuevas reglas a todos los objetos de su organización. Para definir un subconjunto más pequeño de objetivos, seleccione la pestaña **Objetos** e introduzca uno o más **Usuarios**, **Equipos**, **Grupos**, **Unidades de la organización**, o **Endpoints existentes** en las áreas **Incluir** o **Excluir**. El ESM consulta al Directorio activo para verificar los usuarios, equipos, grupos o unidades de la organización, o identifica los endpoints existentes de los mensajes de comunicación anteriores.
Paso 5	(Opcional) Revise el nombre de la regla y la descripción.	La consola ESM genera automáticamente el nombre de la regla y la descripción de acuerdo a los detalles de la regla. Para cancelar el nombre generado automáticamente, seleccione la pestaña **Nombre**, borre la opción **Descripción automática está activada** y, a continuación, introduzca un nombre de regla y la descripción de su elección.
Paso 6	Guarde la regla forense.	Proceda con una de las siguientes opciones: • **Guarde** la regla. Para activar la regla más adelante, seleccione la regla en la página **Políticas > Datos forenses** y haga clic en **Activar**. • **Guarde y aplique** la regla para activarla inmediatamente. Las reglas guardadas aparecen en la página **Políticas > Datos forenses.** Desde ahí, puede **Activar** o **Desactivar** la regla, según sea necesario.

Obtención de datos acerca de un evento de seguridad

Cuando ocurre un evento de seguridad en un endpoint, Traps obtiene datos forenses, incluidos contenidos de memoria y los guarda en el endpoint. Utilice datos forenses para depurar un problema o investigue un problema específico con una aplicación. La selección de esta opción crea una regla de ajustes de agente para recopilar la información obtenida por Traps. Cuando Traps recibe la regla de configuración de agentes, el agente envía todos los logs a la carpeta forense designada.



Para crear una regla general y obtener datos desde un endpoint o más, consulte Gestión de datos recopilados por Traps.

Obtención de datos acerca de un evento de seguridad	
Paso 1	En la consola ESM, seleccione **Eventos de seguridad > Amenazas** para visualizar eventos de seguridad relacionados con procesos protegidos, o **Monitor > Modo provisional** para visualizar eventos de seguridad relacionados con procesos provisionales.
Paso 2	Seleccione el evento de seguridad para el que desea obtener datos. El evento se expande para mostrar detalles y acciones adicionales en relación con el evento de seguridad.
Paso 3	Haga clic en **Obtener**. La consola ESM rellena los ajustes para una regla de configuración de agentes.
Paso 4	Revise los detalles de la regla, y haga clic en **Guardar y aplicar** para activar la regla inmediatamente o **Guardar** para activar. En el siguiente heartbeat, el agente de Traps recibe la nueva regla y envía datos de prevención a la carpeta forense. Para ver el estado de la carga forense, seleccione **Monitor > Obtención de informes forenses**. El agente envía todos los datos relacionados con el evento, incluido un vuelco de memoria del proceso a la carpeta forense designada.
Paso 5	Navegue a la carpeta forense para revisar los datos de prevención.

Habilitación de la obtención de URI en Chrome

A diferencia de otros navegadores, Chrome registra los URI de todas las pestañas de un proceso. Como resultado, debe instalar una extensión de Chrome para habilitar la obtención de URI en Chrome. Esto permite a Traps evitar intentos de explotación en ese navegador. Tras la instalación de la extensión, Chrome registra una devolución para cada solicitud web y registra los URI en un búfer cíclico, de manera similar a los otros mecanismos de obtención de URI de Traps.

Para habilitar la obtención de URI, puede instalar la extensión localmente en un endpoint o usando software de gestión GPO. Las siguientes flujos de trabajo también facilitan pasos para la configuración de la extensión de Chrome en configuraciones online u offline:

- Instalación de la extensión de Chrome en el endpoint
- Instalación de la extensión de Chrome utilizando GPO

Instalación de la extensión de Chrome en el endpoint

Instalación de la extensión de Chrome en el endpoint	
Paso 1	Descargue y extraiga el archivo de extensión Palo Alto Networks Traps Chrome Monitor.

Paso 2	Edite los archivos de extensión:
	• **Online**: Edite la última línea del archivo `Ext.reg` en la ruta exacta del archivo `traps.crx.xml`:
	`"1"="mobnfjmemnepjkflncmogkbnhafgblic;https://clients2.google.com/service/update2/crx"`
	• **Offline**:
	1. Edite la última línea del archivo `Ext.reg` en la ruta exacta del archivo `traps.crx.xml`:
	`"1"="mobnfjmemnepjkflncmogkbnhafgblic;file:c:/....../traps.crx.xml"`
	2. En el archivo `traps.crx.xml`, edite la ruta de `updatecheck codebase` en la ruta exacta del archivo `traps.crx`:
	`<updatecheck codebase='file:c:/ChromeExtension/traps.crx' version='1.4' />`

Paso 3	Guarde y haga doble clic en el archivo reg para la instalación local de forma automática.
Paso 4	Verifique la instalación de la extensión de Chrome: En el navegador Chrome, introduzca `chrome://extensions` y pulse **Intro**. La extensión Palo Alto Networks Traps Chrome Monitor deberá visualizarse en la lista de extensiones.

Instalación de la extensión de Chrome utilizando GPO

Instalación de la extensión de Chrome en el endpoint		
Paso 1	Extraiga los archivos de extensión:	1. Descargue y extraiga el archivo de extensión Palo Alto Networks Traps Chrome Monitor.

Instalación de la extensión de Chrome en el endpoint		
Paso 1	Añada chrome.adm como plantilla en un controlador de dominio.	1. En el escritorio, seleccione **Inicio**, introduzca **gpmc.msc** en el campo de búsqueda y, a continuación, pulse **Intro**. 2. Cree el GPO: En el Administrador de políticas del grupo, seleccione **Bosque > Dominios**. Haga clic con el botón derecho en el dominio y seleccione **Crear GPO en este dominio**. Cambie el nombre del GPO a **TrapsChromeExtention** y haga clic en **Guardar**. 3. Edite el GPO: Haga clic con el botón derecho en el GPP y seleccione **Editar**. Expanda la sección de ajuste del ordenador del GPO. Haga clic en **Políticas > Plantillas administrativas** y haga clic con el botón derecho en **Plantillas administrativas**. Seleccione **Añadir/Eliminar plantillas**. 4. Añada la plantilla de Chrome: Haga clic en **Añadir** y, a continuación, en **Examinar** y haga doble clic en el archivo **chrome.adm**. Se carga el archivo "chrome" en la ventana de plantillas. Haga clic en **Cerrar**.

Paso 2	Añada la plantilla al GPO.	1. En la sección Ajustes del ordenador seleccione **Políticas > Plantillas administrativas > Plantillas administrativas clásicas > Google > Google Chrome** (no ajustes por defecto) **> Extensiones**.
		2. En el lado derecho de la pantalla habrá cinco reglas GPO. Haga doble clic en **Configurar la lista de extensiones instaladas a la fuerza**.
		3. Verifique si el GPO hasta habilitado, y haga clic en **Mostrar** (en el lado izquierdo de la pantalla, en el centro).
		• **Online**: En la fila blanca, introduzca la siguiente cadena:
		`mobnfjmemnepjkflncmogkbnhafgblic;https://clients2.google.com/service/update2/crx`
		• **Offline**: En la fila blanca, introduzca la siguiente cadena (edite el directorio que será la carpeta forense, por ejemplo, //servername/…/forensic):
		`mobnfjmemnepjkflncmogkbnhafgblic;file:c:/…………/traps.crx.xml`
		4. Haga clic en **ACEPTAR**.

Paso 3	Verifique la instalación de la extensión de Chrome:	Abra el navegador Chrome en el endpoint e introduzca `chrome://extensions`. Verifique que la extensión Palo Alto Networks Traps Chrome Monitor aparece en la lista de extensiones.

Informes y logs

El Endpoint Security Manager proporciona informes y logs que son de utilidad para el monitorizado de los endpoints de su organización. Puede monitorizar los logs y filtrar la información para interpretar conductas inusuales en su red. Tras analizar un evento de seguridad, puede crear una regla personalizada para el endpoint o proceso. Los temas siguientes describen cómo visualizar y monitorizar informes sobre el estado de seguridad de los endpoints.

- Mantenimiento de los endpoints y Traps
- Uso del Endpoint Security Manager panel
- Monitorizado de eventos de seguridad
- Monitorizado del estado de los endpoints
- Monitorizado de las reglas
- Monitorización de la obtención de informes forenses
- Monitorización de las notificaciones de los agentes
- Monitorizado de notificaciones del servidor
- Administración de preferencias de informes y logging

Mantenimiento de los endpoints y Traps

De forma diaria o semanal, realice las siguientes acciones:

- Examine el panel para verificar que el agente de Traps está activo en todos los endpoints instalados. Consulte Uso del Endpoint Security Manager panel.
- Examine la página Notificaciones e investigue informes de bloqueos e informes de seguridad. Tras analizar un evento de seguridad, quizás desee realizar cualquiera de las tareas siguientes:
  – Activar la protección para una aplicación desprotegida. Consulte Ver, modificar o borrar un proceso.
  – Deshabilitar temporalmente reglas que interfieren en el trabajo diario. En casos en que un evento de seguridad no indique un ataque y esté interfiriendo con el trabajo diario, puede deshabilitar una regla de prevención o restricción de exploits en un endpoint específico. Consulte Exclusión de un endpoint de una regla de prevención de exploits.
  – Aplicar un parche, actualizar o corregir un error del software que indique una conducta errónea o una vulnerabilidad de seguridad. La aplicación de parches o la actualización de aplicaciones de terceros o la corrección de errores en las aplicaciones que se desarrollan internamente pueden reducir el número de eventos de seguridad enviados al Endpoint Security Manager.
- Revisar procesos desprotegidos en la vista Administración de procesos, y decidir si se habilita la protección en ellos. Consulte Ver, modificar o borrar un proceso.

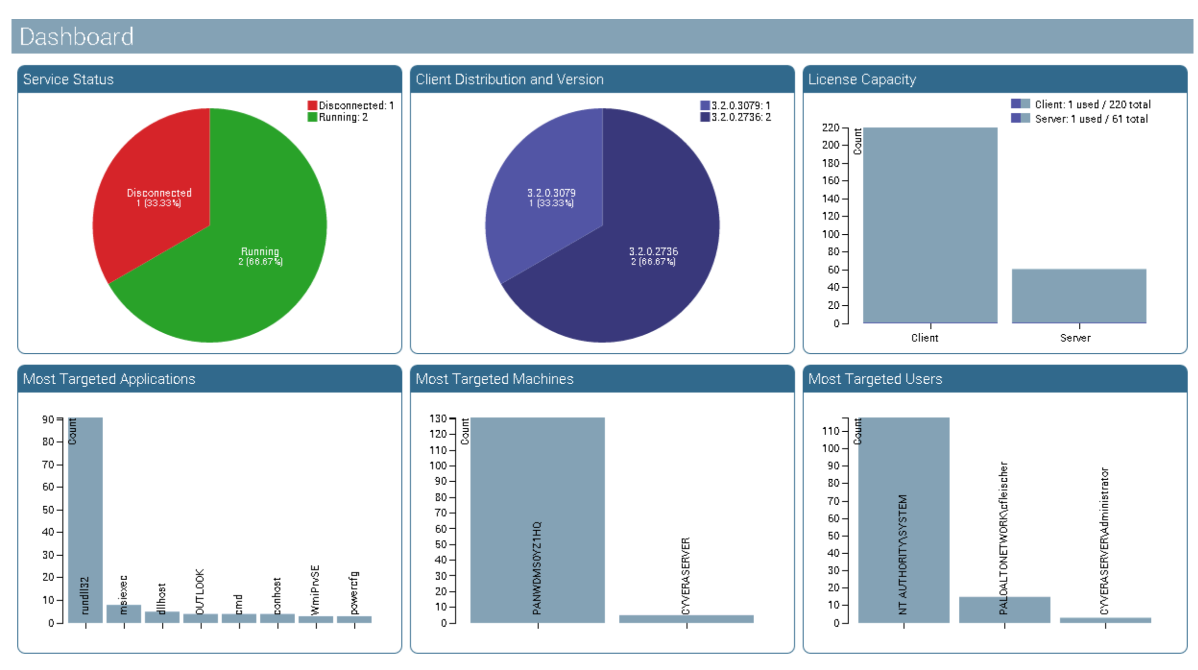
Tras un cambio en la organización o en las versiones disponibles del software Traps, puede:

- Añadir una aplicación de reciente instalación en la lista de procesos protegidos. Consulte Añadir un proceso protegido, provisional o desprotegido.
- Instalar Traps en un nuevo endpoint. Consulte Instalación de Traps en el endpoint.
- Actualizar la versión del agente de Traps en los endpoints. Consulte Desinstalación o actualización de Traps en el endpoint.
- Actualizar la licencia de agentes en los endpoints. Consulte Actualización o revocación de la licencia de Traps en el endpoint.

Uso del Endpoint Security Manager panel

El panel es la primera página que se visualiza tras el inicio de sesión en el Endpoint Security Manager. También puede acceder o actualizar esta página haciendo clic en **Panel** en el menú superior.

El panel muestra varios cuadros que presentan estadísticas relacionadas con instancias de agentes de Traps. El panel no es configurable.



La siguiente tabla describe cada cuadro:

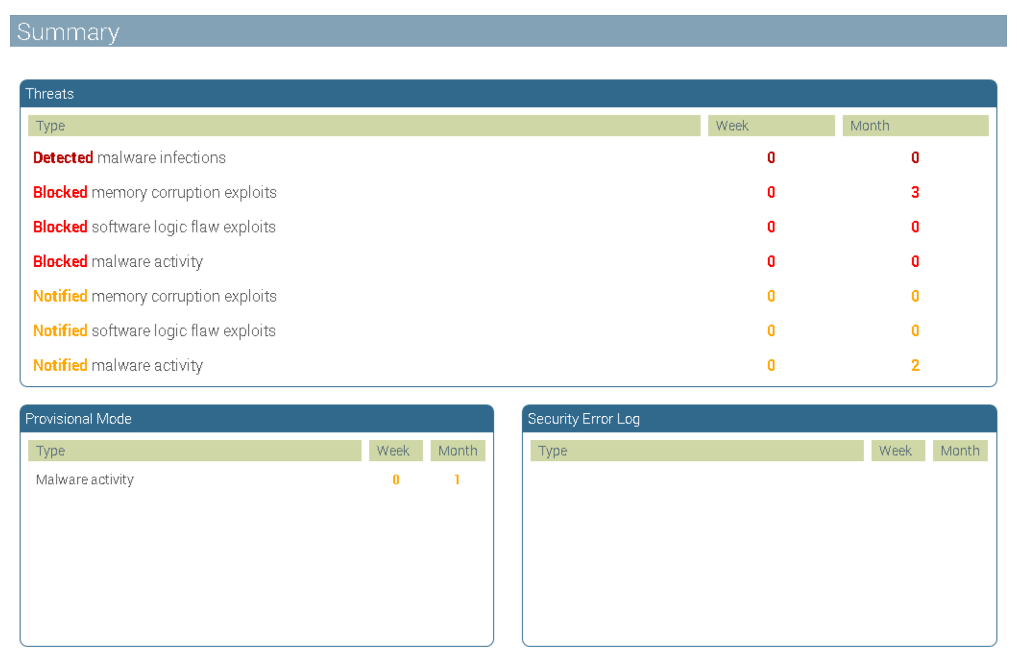
Cuadro del panel	Descripción
Estado de servicio	Muestra el estado de las instancias de agentes de Traps instalados en los endpoints por número y porcentaje. Los posibles estados son: • **Ejecución**—El agente se está ejecutando. • **Parado**—Se ha detenido el servicio del agente. • **Desconectado**—El servidor no ha recibido un mensaje heartbeat del agente durante un tiempo preconfigurado. • **Cierre**—Se ha cerrado el endpoint.
Distribución y versión de clientes	Muestra la versión de las instancias de agentes de Traps instalados en los endpoints por número y porcentaje.
Capacidad de licencias	Muestra la utilización de las licencias de Traps para el servidor y el cliente por número de licencias utilizadas y disponibles.
Aplicaciones más atacadas	Muestra las aplicaciones que tienen la cantidad más alta de prevenciones.
Máquinas más atacadas	Muestra los endpoints que tienen la distribución más alta de prevenciones.
Usuarios más atacados	Muestra los prevenciones que tienen la distribución más alta por usuario final.

Monitorizado de eventos de seguridad

Utilice la página Eventos de seguridad y sus pestañas para administrar alertas y detectar nuevas amenazas.

- Uso del panel de eventos de seguridad
- Ver el historial de eventos de seguridad en un endpoint
- Exclusión de un endpoint de una regla de prevención de exploits

Uso del panel de eventos de seguridad



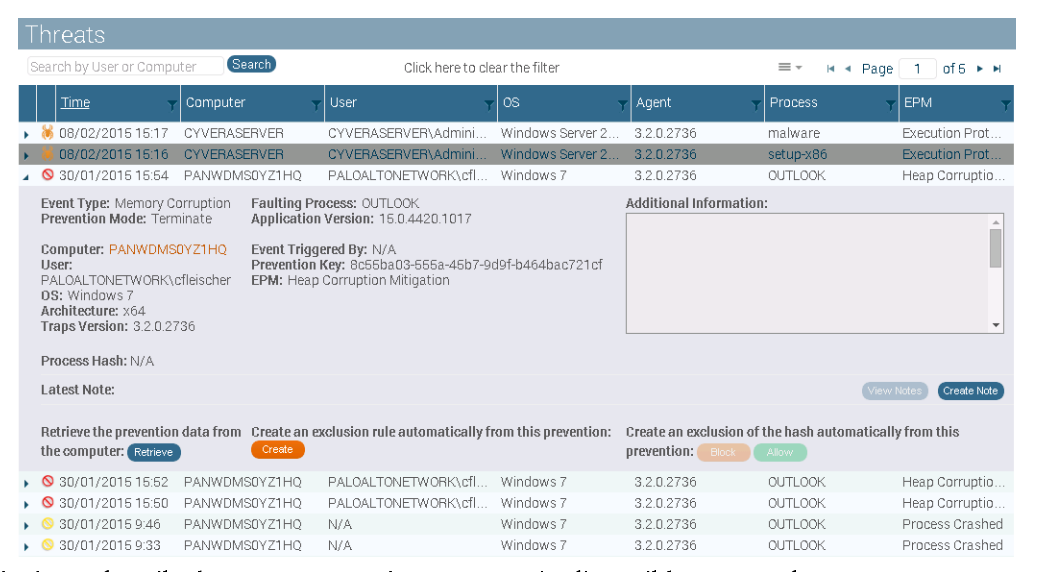
Utilice el panel **Eventos de seguridad** para monitorizar la información de alto nivel acerca de eventos de seguridad que ocurren en los endpoints de su organización. Desde aquí puede ver el número de eventos que han ocurrido en la última semana o mes. El panel de eventos de seguridad muestra los eventos en los que se han bloqueados intentos de exploits y eventos que han activado solo notificaciones. El panel muestra la información siguiente:

Componente del panel	Descripción
Amenazas	Muestra todas las amenazas en relación con procesos protegidos y ejecutables que se han producido en su red. Para una mayor comodidad, haga clic en cualquier tipo de amenaza mostrado en la página **Resumen** para filtrar las amenazas de ese tipo. Para obtener más información, consulte Ver detalles de amenazas.

Componente del panel	Descripción
Modo provisional	El área **Modo provisional** del panel **Eventos de seguridad** incluye un resumen de alto nivel de los eventos relacionados con reglas provisionales. Haga clic en un evento del área **Modo provisional** para saltar a una vista filtrada de la página **Monitor > Modo provisional** para eventos de ese tipo. Por defecto, la página **Modo provisional** muestra eventos relacionados con los módulos siguientes: • ProcesoBloqueo • WildFireDesconocido • WildFirePostDesconocidoDetección • Protección de secuestro de DLL • Java • Inyección de subprocesos • Protección de suspensión Para obtener más información, consulte Ver detalles de modo provisionales.
Log de errores de seguridad	Muestra todos los errores y problemas recientes que los que informan los endpoints de su organización. Haga clic en cualquier tipo de error en la página **Resumen** para realizar una filtración por errores de ese tipo. Para obtener más información, consulte Ver detalles de log de errores de seguridad.

Ver detalles de amenazas

Seleccione **Eventos de seguridad > Amenazas** para visualizar una lista de las amenazas que han ocurrido en su red. Desde esta página puede ver detalles relacionados con eventos de seguridad, crear y ver notas acerca del evento, recuperar datos de logs acerca del evento del endpoint, o crear una regla de exclusión para permitir la ejecución del proceso en un endpoint particular. Por defecto, la vista de detalles estándar de la página Amenazas ofrece una tabla de eventos de seguridad con campos mostrados a lo largo de la parte superior. Al seleccionar un evento en la tabla Amenazas se expande la hilera para mostrar detalles adicionales en relación con el evento de seguridad. También puede exportar los logs a un archivo CSV haciendo clic en el icono del menú ≡ ▾, y seleccionando **Exportar logs**.



La tabla siguiente describe los campos y acciones que están disponibles para cada amenaza.

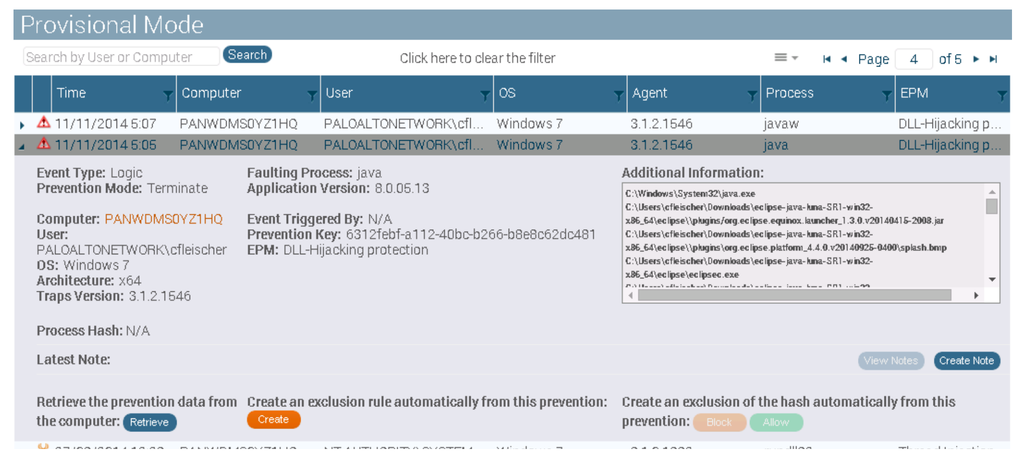
Campo	Descripción
Vista de detalles estándar	
Hora	La fecha y hora a la que se ha producido la prevención.
Equipo	El nombre de host del endpoint en el que ha ocurrido el evento de prevención.
Usuario	El nombre del usuario bajo el que se está ejecutando el proceso (que ha causado el evento).
SO	El sistema operativo instalado en el endpoint.
Agente (versión de Traps)	El versión de Traps instalada en el endpoint.
Proceso	El nombre del proceso que ha causado el evento.
EPM	El Módulo de prevención de exploits (EPM) o la regla de restricción que ha activado la prevención.
Vista de detalles adicionales	
Tipo de evento	Tipo de amenaza, detección de mensajes de WildFire, lógica, malware, acciones sospechosas o corrupción de memoria.
Modo de prevención	Acción que realiza la regla, terminar el proceso o información al usuario.
Arquitectura	Tipo de arquitectura del sistema operativo (SO). Por ejemplo, x64.
Clave de prevención	Identificador único para el evento de seguridad. Cuando se obtienen datos acerca de un evento, Traps crea una clave de log utilizando esa clave de prevención como el nombre del archivo.
Desencadenador	Archivo o archivos que activan un evento de seguridad.
Botón **Ver notas**	Visualiza notas acerca del evento de seguridad. Si no hay notas, está opción queda oscurecida.
Botón **Crear nota**	Crea notas acerca del evento de seguridad para el seguimiento en un momento o fecha posteriores.
Botón **Obtener**	Obtiene los datos de protección del endpoint. Crea una regla que utiliza la clave de prevención y activa información para solicitar datos acerca del evento de prevención del agente. La información se envía a la carpeta forense.
Botón **Crear**	Crea una regla de exclusión automáticamente a partir de una prevención. La regla permite la ejecución de una regla en un endpoint específico sin la protección del modo de prevención de exploits.
Botón **Bloquear**	(Solo prevenciones de WildFire) Cancela el modo de terminación por defecto para que el hash bloquee el archivo.
Botón **Permitir**	(Solo prevenciones de WildFire) Cancela el modo de terminación por defecto para que el hash permita el archivo.

Seleccione la lista de nuevo para ocultar la vista de detalles adicionales.

Ver detalles de modo provisionales

Seleccione **Monitor > Modo provisional** para mostrar una lista de eventos de seguridad relacionados con módulos provisionales. Los módulos provisionales se configuran por defecto e incluyen ProcessCrash, WildFireUnknown, WildFirePostUnknownDetection, protección contra secuestro de DLL, Java, Inyección de subprocesos y Protección de suspensión.

Desde la página **Modo provisional** puede ver detalles relacionados con eventos de seguridad, crear y ver notas acerca del evento, recuperar datos de logs acerca del evento del endpoint, o crear una regla de exclusión para permitir la ejecución del proceso en un endpoint particular. Por defecto, la vista de detalles estándar de la página **Modo provisional** ofrece una tabla de eventos de seguridad con campos mostrados a lo largo de la parte superior. Al seleccionar un evento en la tabla Modo provisional se expande la hilera para mostrar detalles adicionales en relación con el evento de seguridad. También puede exportar los logs a un archivo CSV haciendo clic en el icono del menú ≡ ▾, y seleccionando **Exportar logs**.



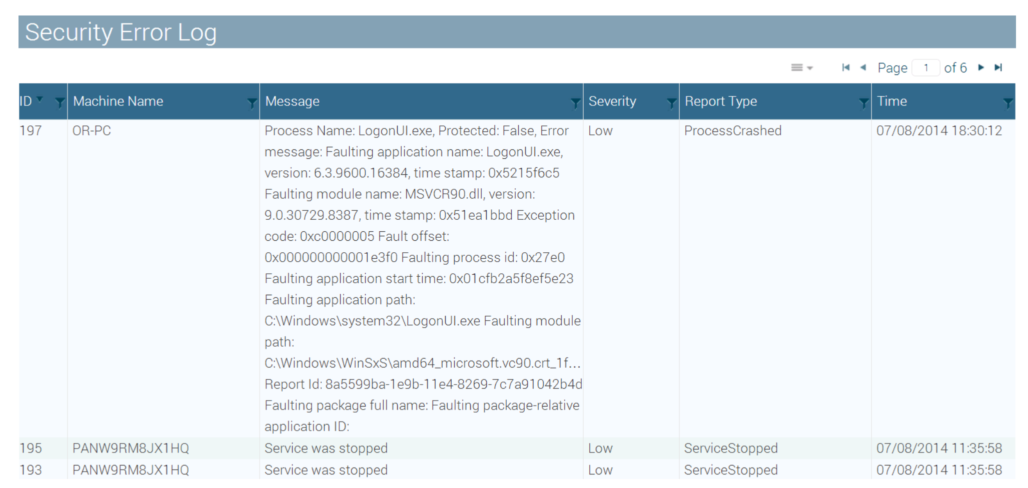
La tabla siguiente describe los campos y acciones que están disponibles para cada evento de seguridad en modo provisional.

Campo	Descripción
Vista de detalles estándar	
Hora	La fecha y hora a la que se ha producido la prevención.
Equipo	El nombre del endpoint en el que ha ocurrido el evento de prevención.
Usuario	El nombre del usuario bajo el que se está ejecutando el proceso (que ha causado el evento).
SO	El sistema operativo instalado en el endpoint.
Agente (versión de Traps)	El versión de Traps instalada en el endpoint.
Proceso	El nombre del proceso que ha causado el evento.
EPM	El Módulo de prevención de exploits (EPM) o la regla de restricción que ha activado la prevención.
Vista de detalles adicionales	
Tipo de evento	Tipo de amenaza, detección de mensajes de WildFire, lógica, malware, acciones sospechosas o corrupción de memoria.

Campo	Descripción
Modo de prevención	Acción que realiza la regla, terminar el proceso o información al usuario.
Arquitectura	Tipo de arquitectura del sistema operativo (SO). Por ejemplo, x64.
Clave de prevención	Clave única asociada con el evento de prevención. Cuando se obtienen datos acerca de un evento, Traps crea una clave de log utilizando esa clave de prevención como el nombre del archivo.
Desencadenador	Archivo o archivos que activan un evento de seguridad.
Botón **Ver notas**	Visualiza notas acerca del evento de seguridad. Si no hay notas, está opción queda oscurecida.
Botón **Crear nota**	Crea notas acerca del evento de seguridad para el seguimiento en un momento o fecha posteriores.
Botón **Obtener**	Obtiene los datos de protección del endpoint. Crea una regla que utiliza la clave de prevención y activa información para solicitar datos acerca del evento de prevención del agente. La información se envía a la carpeta forense.
Botón **Crear**	Crea una regla de exclusión automáticamente a partir de una prevención. La regla permite la ejecución de una regla en un endpoint específico sin la protección del modo de prevención de exploits.
Botón **Bloquear**	(Solo prevenciones de WildFire) Cancela el modo de terminación por defecto para que el hash bloquee el archivo.
Botón **Permitir**	(Solo prevenciones de WildFire) Cancela el modo de terminación por defecto para que el hash permita el archivo.

Ver detalles de log de errores de seguridad

Seleccione **Seguridad Eventos > Log de errores de seguridad** para mostrar eventos de seguridad relacionados con la conducta del agente y la seguridad del endpoint. El evento incluye cambios en el servicio, como el inicio o parada de un servicio. En raras ocasiones, el log de errores de seguridad también puede mostrar problemas encontrados durante la protección de un proceso en el que falla o se bloquea la inyección.


Security Error Log

Page 1 of 6

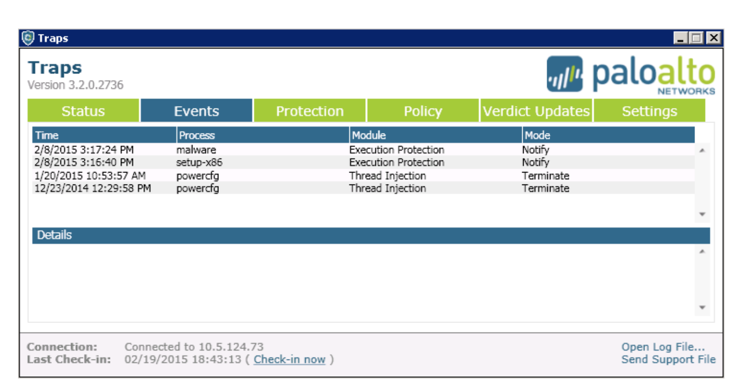
ID	Machine Name	Message	Severity	Report Type	Time
197	OR-PC	Process Name: LogonUI.exe, Protected: False, Error message: Faulting application name: LogonUI.exe, version: 6.3.9600.16384, time stamp: 0x5215f6c5 Faulting module name: MSVCR90.dll, version: 9.0.30729.8387, time stamp: 0x51ea1bbd Exception code: 0xc0000005 Fault offset: 0x000000000001e3f0 Faulting process id: 0x27e0 Faulting application start time: 0x01cfb2a5f8ef5e23 Faulting application path: C:\Windows\system32\LogonUI.exe Faulting module path: C:\Windows\WinSxS\amd64_microsoft.vc90.crt_1f... Report Id: 8a5599ba-1e9b-11e4-8269-7c7a91042b4d Faulting package full name: Faulting package-relative application ID:	Low	ProcessCrashed	07/08/2014 18:30:12
195	PANW9RM8JX1HQ	Service was stopped	Low	ServiceStopped	07/08/2014 11:35:58
193	PANW9RM8JX1HQ	Service was stopped	Low	ServiceStopped	07/08/2014 11:35:58

La tabla siguiente describe los campos mostrados en el log de errores de seguridad.

Campo	Descripción
ID	Número de ID único asociado con el error de seguridad.
Nombre de la máquina	Nombre del endpoint en el que ha ocurrido el evento de prevención.
Mensaje	Texto de mensaje de notificación.
Gravedad	La gravedad del error, que depende del tipo de informe: • **Alta** • **Media** • **Baja**
Tipo de informe	El tipo del error que ha activado la notificación. Los valores posibles son: • **Estado de realización de acciones de una vez**—Una acción realizada en el endpoint La gravedad es baja si se completa la acción, o media si falla la acción. • **Bloqueo de proceso**—Un proceso bloqueado en el endpoint. Gravedad baja. • **Inyección de proceso agotada**—Se ha agotado la inyección al proceso. Gravedad media. • **Servicio vivo**—Se ha iniciado el servicio del agente. Gravedad baja. • **Servicio parado**—Se ha parado el servicio del agente. Gravedad baja. • **Sistema cerrado**—Se ha cerrado el endpoint. Gravedad baja. • **Acceso DEP no asignado**—Un salto del puntero de instrucciones a una localización no asignada en la memoria. Suele deberse a un error de aplicación, pero también podría indicar un intento (fallido) de exploit. Gravedad media. • **Fallo de inicio de servicio de información nativa**—Ha fallado el servicio de información. Gravedad alta.
Hora	Fecha y hora a las que Traps ha informado del error.

Ver el historial de eventos de seguridad en un endpoint

Cuando un usuario activa un proceso en el endpoint, Traps inyecta un módulo de protección, conocido como Módulo de prevención de exploits (EPM), en el proceso. Las reglas de las políticas de seguridad de endpoints determinan los EPM que se inyectan en cada proceso. Durante la inyección, aparece el nombre del proceso en rojo en la consola. Cuando se ha realizado la inyección con éxito, la consola elabora un log del evento del seguridad en la pestaña **Eventos** .



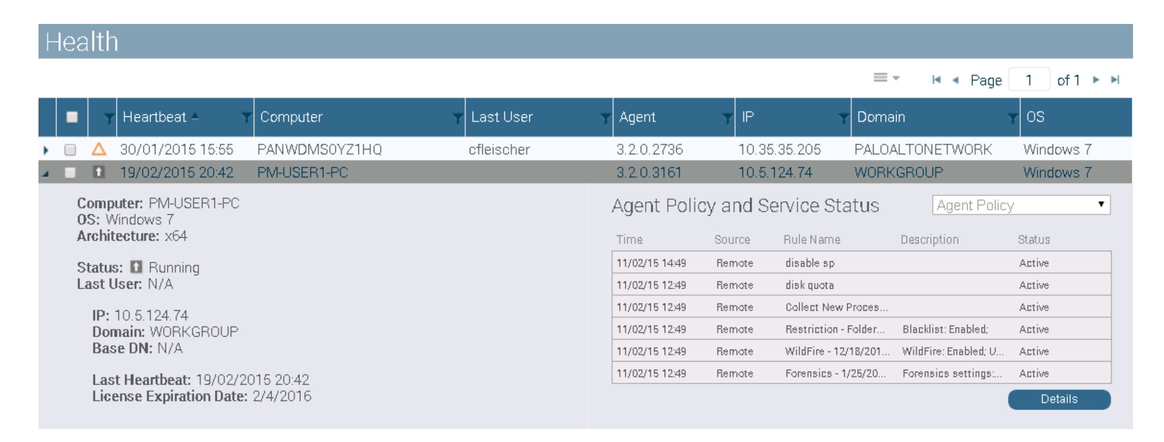
Cada uno de los eventos de la pestaña **Eventos** muestra la fecha y la hora del evento, el nombre del proceso afectado y el EPMS que se ha inyectado en el proceso. Normalmente, el modo indica si Traps ha finalizado o no el proceso o si solo ha informado al usuario acerca del evento.

Ver el historial de eventos de seguridad en un endpoint	
Paso 1	Inicie la consola de Traps: • En la bandeja de Windows, haga clic con el botón derecho en el icono de Traps y seleccione la **Consola**, o haga doble clic en el icono. • Ejecute CyveraConsole.exe desde la pantalla de instalación de Traps. Se inicia la consola de Traps.
Paso 2	Se muestran los eventos de seguridad: 1. Seleccione **Avanzado > Eventos** para visualizar los eventos de seguridad del endpoint. 2. Utilice las flechas ascendente y descendente para desplazarse a través de la lista de eventos.

Monitorizado del estado de los endpoints

Ver detalles de estado de los endpoints

Desde la consola ESM, seleccione **Monitorizar > Estado** para mostrar una lista de los endpoints de la organización y el correspondiente estado de seguridad.



La tabla siguiente describe los campos y acciones que están disponibles para cada endpoint mostrado en la página **Estado**. Por defecto, la vista de detalles estándar de la página Estado ofrece una tabla de endpoints con campos mostrados a lo largo de la parte superior. Al seleccionar un endpoint en la tabla Estado se expande la fila para mostrar detalles adicionales acerca del endpoint y las acciones que se pueden realizar. También puede exportar los logs a un archivo CSV haciendo clic en el icono del menú ≡ ▾, y seleccionando **Exportar logs**.

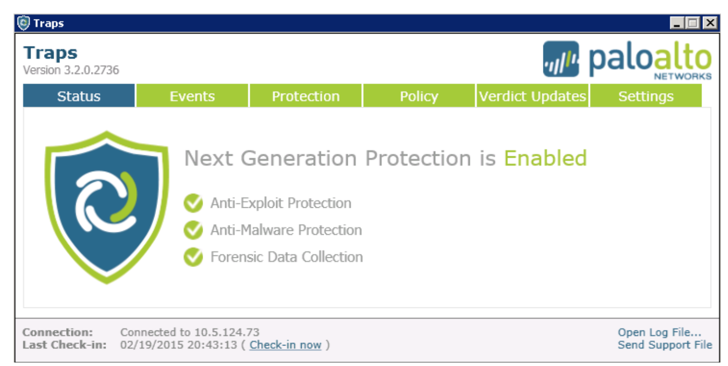
Campo	Descripción
Vista de detalles estándar	
Estado	El estado del agente, que es **En ejecución**, **Parado**, **Desconectado** o **Cerrado**.
Heartbeat	La fecha y la hora a la que se ha enviado el último mensaje heartbeat desde el agente.
Equipo	El nombre del endpoint.
Último usuario	El nombre del último usuario que ha iniciado sesión en el endpoint.
Agente	La versión del agente de Traps instalado.
IP	La dirección IP del endpoint.

Campo	Descripción
Dominio	El nombre del dominio del endpoint.
SO	El sistema operativo instalado en el endpoint.
Vista de detalles adicionales	
Arquitectura	Tipo de arquitectura del sistema operativo (SO). Por ejemplo, x64.
Último heartbeat	Fecha y hora del servidor que se ha comunicado por última vez con Traps.
Fecha de vencimiento de licencia	Fecha en la que vence la licencia del endpoint.
DN base	Ruta del Protocolo ligero de acceso a directorios (LDAP) del endpoint.
Botón **Detalles**	Seleccione **Política de agentes** o logs **Estado de servicio** de la lista desplegable y haga clic en **Detalles** para revisar la lista completa para el endpoint. Para más información, consulte Ver el historial de reglas de un endpoint y Ver el historial de estado de servicio de un endpoint.

Seleccione la lista de nuevo para ocultar la vista de detalles adicionales.

Ver detalles de estado de Traps

La consola muestra los servicios activos e inactivos mostrando un ✅ o ❌ a la izquierda del tipo de servicio. Seleccione la pestaña **Avanzado** para mostrar pestañas adicionales a lo largo de la parte superior de la consola. Las pestañas le permiten navegar a páginas que muestran detalles adicionales acerca de eventos de seguridad, procesos protegidos y actualizaciones para la política de seguridad. Normalmente, un usuario no necesita ejecutar la consola de Traps, pero la información puede ser de utilidad cuando se investiga un evento relacionado con la seguridad. Se puede decidir ocultar el icono de la bandeja de la consola que activa la consola, o evitar su activación. Para obtener más información, consulte Ocultación o restricción de acceso a la consola de Traps.



Elemento del sistema	Descripción
Protección anti exploits	Indica si se activan o no las reglas de prevención de exploits en la política de seguridad de endpoints.
Protección antimalware	Indica si se activan o no los módulos de restricción y/o prevención de malware en la política de seguridad de endpoints.

Elemento del sistema	Descripción
Recopilación de datos forenses	Indica si se ha habilitado o no la integración de WildFire.
Pestaña **Estado**	Muestra el estado de **Conexión** y el nivel de protección del endpoint. La consola Traps abre la pestaña **Estado** por defecto.
Pestaña **Eventos**	Muestra eventos de seguridad que se han producido en el endpoint.
Pestaña **Protección**	Muestra los procesos que protege el agente de Traps que están en ejecución en el endpoint.
Pestaña **Política**	Muestra cambios en la política de seguridad de endpoints incluidas la fecha y hora de la actualización.
Pestaña **Actualizaciones de veredictos**	Muestra los cambios en el veredicto para ejecutables que se han abierto en el endpoint.
Configuración	Muestra las opciones de idioma que se pueden usar para cambiar el idioma de la consola de Traps.
Enlace **Registrar ahora**	Inicia una actualización inmediata de la política de seguridad.
Conexión	Muestra el estado de la conexión entre Traps y el servidor ESM.
Último registro	Muestra la fecha y la hora a la que Traps ha recibido por última vez un mensaje heartbeat.
Abrir archivo de registro.	Abre el archivos de seguimiento más reciente del endpoint.
Enviar archivo de soporte	Crea un archivo comprimido de rastros y lo envía a la carpeta forense.

Ver el historial de reglas de un endpoint

Por defecto, la vista de detalles estándar de la página **Estado** ofrece una tabla de endpoints con campos mostrados a lo largo de la parte superior. La selección de un endpoint de la tabla Estado expande la fila para mostrar detalles adicionales acerca del endpoint y le permite ver el historial de reglas de objetos de su organización. Cada regla de la política de agentes muestra la fecha y hora de aplicación de la regla por parte de Traps, la fuente de la regla de política (local o remota), el nombre y descripción de la regla, y el estado actual de esa regla.

Ver el historial de reglas de un endpoint	
Paso 1	Abra el Endpoint Security Manager y seleccione **Monitorizar > Salud**.
Paso 2	Seleccione la fila del endpoint para el que desea visualizar el historial de reglas. La fila se expande para mostrar detalles y acciones adicionales que se pueden realizar.
Paso 3	Seleccione **Política de agentes** en la lista desplegable de la derecha. Aparece la información de estado actual en el sección Política de agentes y logs de la página.
Paso 4	Haga clic en **Detalles** para ver el registro del historial de reglas. El estado indica uno de los siguientes: • **Activa**—La regla está activa en la política de seguridad del endpoint. • **Histórica**—La regla es un versión anterior de una regla que está activa en la política de seguridad del endpoint. • **Deshabilitada**—La regla estaba desactivada en la política de seguridad.

Ver cambios en la política de seguridad del endpoint

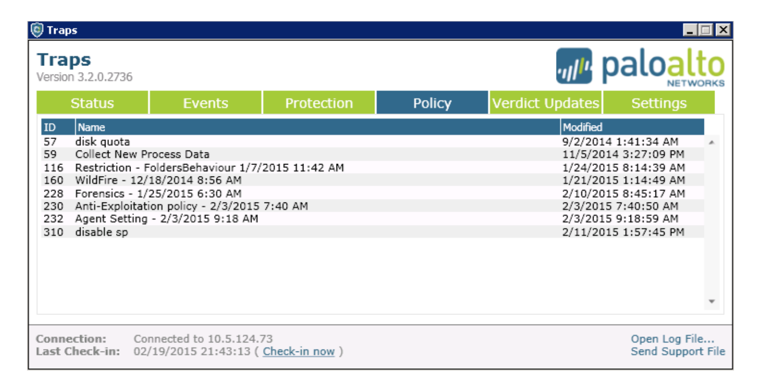
La pestaña **Política** de la consola de Traps muestra cambios en la política de seguridad del endpoint. Cada norma muestra el número de ID único, el nombre de la regla, la fecha y hora en que Traps ha recibido la política de seguridad actualizada que contiene la regla, y la descripción.



Cada tipo de regla tiene una página de administración dedicada que se puede usar para ver y administrar las reglas para la organización. Para crear un archivo de texto que contenga la política de seguridad activa en un endpoint, ejecute lo siguiente desde una línea de comando:

cyveraconsole.exe export(641980) c:\{TargetFolder}\policy.txt

Ver cambios en la política de seguridad del endpoint	
Paso 1	Proceda de una de las maneras siguientes para activar la consola de Traps en el endpoint: • En la bandeja de Windows, haga clic con el botón derecho en el icono de Traps y seleccione la **Consola**, o haga doble clic en el icono. • Ejecute CyveraConsole.exe desde la carpeta de instalación de la consola de Traps.
Paso 2	Ver los eventos de seguridad: 1. Si es necesario, haga clic en **Avanzado** para mostrar pestañas adicionales. A continuación, haga clic en la pestaña **Política** para mostrar las reglas de protección que se están ejecutando en el endpoint. 2. Utilice las flechas ascendente y descendente para desplazarse a través de la lista de reglas de protección.



Ver el historial de estado de servicio de un endpoint

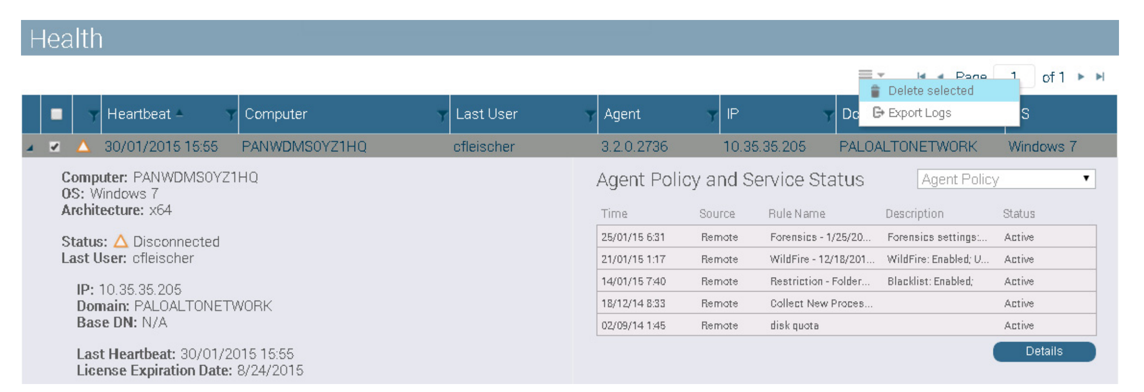
Por defecto, la vista de detalles estándar de la página **Estado** ofrece una tabla de endpoints con campos mostrados a lo largo de la parte superior. La selección de un endpoint de la tabla Estado expande la fila para mostrar detalles adicionales acerca del endpoint y le permite ver el historial del estado del agente de Traps en el endpoint. Una lista desplegable de la sección Política de agentes y estado de servicio le permite visualizar una lista parcial de eventos del **Estado de servicio**. En esta sección también puede ver el log del historial completo del estado de servicio. Cada evento del log muestra la fecha y la hora del cambio de servicio, la versión de Traps que se está ejecutando en el endpoint y el cambio del estado, desconectado, en ejecución, cerrado o parado.

Ver el historial de estado de servicio de un endpoint	
Paso 1	En la consola ESM, seleccione **Monitorizar > Estado**.

Ver el historial de estado de servicio de un endpoint (Continuación)	
Paso 2	Seleccione la fila del endpoint para el que desea visualizar el historial de reglas. La fila se expande para mostrar detalles y acciones adicionales que se pueden realizar.
Paso 3	Seleccione **Estado de servicio** en la lista desplegable de la derecha. Aparece la información de estado actual en el sección Política de agentes y logs de la página.
Paso 4	Haga clic en **Detalles** para ver el log del historial completo del estado de servicio.

Eliminación de un endpoint de la página de estado

La página **Estado** muestra una tabla de todos los endpoints que se han conectado con éxito al Endpoint Security Manager. En situaciones en las que se debe eliminar uno o más endpoints del Endpoint Security Manager, por ejemplo, para limpiar duplicados o eliminar endpoints que ya no se usan, puede utilizar la opción **Borrar seleccionado** del menú de la parte superior de la tabla.

Eliminación de un endpoint de la página de estado	
Paso 1	En la consola ESM, seleccione **Monitorizar > Estado**.
Paso 2	Seleccione la fila o filas del endpoint o endpoints para lo que desea borrar.
Paso 3	Seleccione **Borrar seleccionados** en el menú ≡ ▾ de la parte superior de la tabla Estado. Haga clic en **OK** para confirmar que desea borrar.  La consola ESM elimina el endpoint o endpoints de la página **Estado**. Tras la comunicación heartbeat al endpoint, Traps informa de **Sin conexión al servidor**.

Monitorizado de las reglas

Cada resumen de reglas y página de administración muestra reglas activas e inactivas para su organización y tienen herramientas que se pueden usar para la administración de las reglas.

▲ Ver el resumen de reglas

▲ Ver detalles acerca de las reglas

Ver el resumen de reglas

Cada tipo de regla tiene un resumen específico y una página de administración. Para visualizar un resumen de las reglas de un determinado tipo:

Ver el resumen de reglas	
Paso 1	En la consola ESM, seleccione la página de administración de reglas para ese tipo de regla, por ejemplo, **Políticas > Exploit > Módulos de protección**.
Paso 2	Para visualizar las entrada de la tabla, utilice los controles de paginado de la parte superior derecha de cada página para ver diferentes partes de la tabla.
Paso 3	(Opcional) Para ordenar las entradas de las tablas, seleccionado el encabezado de la columna para aplicar un orden ascendente. Seleccione el encabezado de la columna de nuevo para aplicar un orden descendente.
Paso 4	(Opcional) Para filtrar las entradas de la tabla, haga clic en el icono del filtro a la derecha de la columna para especificar hasta dos conjuntos de criterios para la filtración de los resultados.
Paso 5	(Opcional) Para expandir una entrada de regla, haga clic en la flecha de expansión del lado derecho de la regla. En la vista expandida puede ver los detalles de las reglas adicionales o realizar cualquier acción para administrar una regla. Consulte Guardar reglas.

Ver detalles acerca de las reglas

Cada resumen de regla y página de administración de la consola ESM muestra detalles acerca de las reglas que incluye la política de seguridad de su organización.

La tabla siguiente describe los campos y acciones disponibles para cada página de administración de reglas, incluidos la prevención de exploits, prevención de malware, restricción, ajustes de WildFire, acción , ajustes de agentes y reglas forenses. La vista de detalles estándar proporciona información resumida para cada regla y muestra una tabla de reglas con campos mostrados a lo largo de la parte superior. Al seleccionar una regla de la tabla se expande la fila para mostrar detalles adicionales acerca de la regla y las acciones que se pueden realizar.

Campo	Descripción
Vista de detalles estándar	
ID	Una ID numérica única para la regla.
Estado	• —Activa • —Inactiva

Campo	Descripción
Tipo	• **Protección contra exploits** • **Restricción** • **Protección de malware** • **WildFire** • **Acción de agente** • **Ajuste de agente** • **Datos forenses**
Fecha modificada	La fecha y la hora de creación o última modificación de la regla.
Nombre	El nombre de la regla.
Descripción	La descripción de la regla.
Asociado	Los objetos de destino a los que se aplica la regla.
Condición	Las condiciones que deben cumplirse (si las hay) para aplicación de la regla.
Vista de detalles adicionales	
Creador	El usuario que ha creado la regla.
Creado	La fecha y hora de creación de la regla.
Modificador	La cuenta de usuario que ha modificado la regla por última vez, si se conoce.
Procesos	(Solo reglas de prevención de exploits) Los procesos de destino de la regla.
EPM	(Solo reglas de prevención de exploits) El Módulo de prevención de exploits (EPM) que protege el proceso.
Acción de una vez	(Solo reglas de acción) La acción que se va a realizar en el endpoint.
Restricciones	(Solo reglas de restricción) El método de restricción que protege contra ejecutables maliciosos.
Ajustes de agentes	(Solo reglas de ajustes de agentes) La acción que se va a realizar en el software Traps.
Duplicar	(Solo reglas de acción) Vuelve a ejecutar la regla de acción.
Borrar	Borra la regla.
Activar	Activa la regla (solo reglas inactivas).
Desactivar	Desactiva la regla (solo reglas activas).
Editar	Edita la regla (solo reglas de prevención de exploits, restricción y ajustes de agentes).

Monitorización de la obtención de informes forenses

En la página **Monitorizado > Obtención de informes forenses**, puede visualizar información acera de los archivos de datos forenses, actualizaciones de WildFire, y obtención de volcados de memoria, y administración de archivos de datos desde una localización central.

La tabla siguiente describe los campos y acciones que están disponibles para cada archivo de datos forenses. La página **Obtención de informes forenses** muestra una tabla con los campos visualizados a lo largo de la parte superior y acciones que se pueden realizar para administrar la obtención de informes forenses.

Campo	Descripción
Nombre de archivo	Una ID numérica única para la regla.
Estado de la carga	Estado de la carga, por ejemplo, **Fallido**, **En curso**, etc.
Nombre de la máquina	Nombre de la máquina desde la que se han obtenido los datos forenses.
Tipo de archivo	Tipo de datos forenses, por ejemplo, logs, WildFire o volcado.
Tamaño de archivo	Tamaño del archivo forense.
Fecha de creación	La fecha y la hora de creación o última modificación de la regla de obtención.
Botón **Descargar**	Descarga el archivo de datos forenses.
Botón Borrar	Borra el archivo de datos forenses.

Se pueden ordenar las entradas de la tabla en orden ascendente seleccionando el encabezado de la columna. Seleccione el encabezado de nuevo para ordenar las entradas de la tabla en orden descendente. Para limitar los resultados, haga clic en el icono de filtración a la derecha de la columna y especifique hasta dos conjuntos de criterios. También puede exportar los logs a un archivo CSV haciendo clic en el icono del menú, y seleccionando **Exportar logs**.

Monitorización de las notificaciones de los agentes

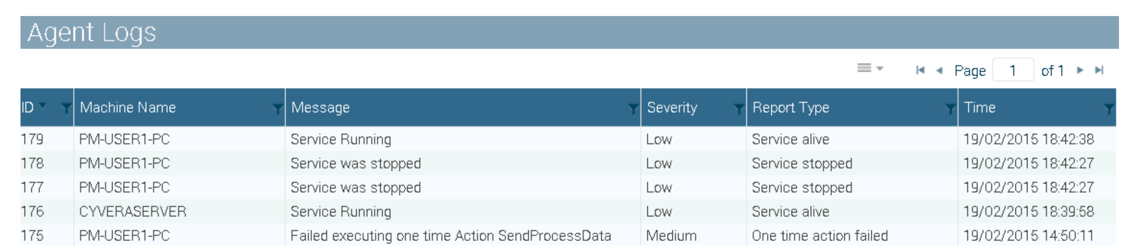
Ver notificaciones acerca de cambios en el estado de agentes

Utilice la página **Logs de agentes** para visualizar notificaciones acerca de los cambios en el estado de los agentes, incluido el inicio o parada de los servicios, sistemas y procesos.

Ver notificaciones acerca de cambios en el estado de agentes	
Paso 1	En la consola ESM, seleccione **Monitorizar > Logs de agentes**.
Paso 2	Para visualizar las entrada de la tabla, utilice los controles de paginado de la parte superior derecha de cada página para ver diferentes partes de la tabla.
Paso 3	(Opcional) Para ordenar las entradas de las tablas, seleccione el encabezado de la columna para aplicar un orden ascendente. Seleccione el encabezado de la columna de nuevo para aplicar un orden descendente.
Paso 4	(Opcional) Para filtrar las entradas de la tabla, haga clic en el icono del filtro a la derecha de la columna para especificar hasta dos conjuntos de criterios para la filtración de los resultados.
Paso 5	(Opcional) Para exportar los logs a un archivo CSV, haga clic en el icono de menú y, a continuación, seleccione **Exportar logs**.

Ver detalles acerca del registro de agentes

La página **Logs de agentes** muestra notificaciones acerca de los cambios en el estado de los agentes, incluido el inicio o parada de los servicios, sistemas y procesos.



Agent Logs

Page 1 of 1

ID	Machine Name	Message	Severity	Report Type	Time
179	PM-USER1-PC	Service Running	Low	Service alive	19/02/2015 18:42:38
178	PM-USER1-PC	Service was stopped	Low	Service stopped	19/02/2015 18:42:27
177	PM-USER1-PC	Service was stopped	Low	Service stopped	19/02/2015 18:42:27
176	CYVERASERVER	Service Running	Low	Service alive	19/02/2015 18:39:58
175	PM-USER1-PC	Failed executing one time Action SendProcessData	Medium	One time action failed	19/02/2015 14:50:11

La tabla siguiente describe los campos mostrados en la página **Monitorizar > Logs de agentes**.

Campo	Descripción
ID	Una ID numérica única para el mensaje de notificación.
Nombre de la máquina	El nombre del endpoint que ha producido la notificación.
Mensaje	El texto de mensaje de notificación.

Campo	Descripción
Gravedad	La gravedad de la notificación, que depende del tipo de informe: • **Alta** • **Media** • **Baja**
Tipo de informe	El tipo del evento que ha activado la notificación. • **Estado de realización de una acción de una vez**—Una acción realizada en el endpoint. La gravedad es baja si se completa la acción, o media si falla la acción. • **Bloqueo de proceso**—Un proceso bloqueado en el endpoint. Gravedad baja. • **Inyección de proceso agotada**—Se ha agotado la inyección al proceso. Gravedad media. • **Servicio vivo**—Se ha iniciado el servicio del agente. Gravedad baja. • **Servicio detenido**—Se ha detenido el servicio del agente. Gravedad baja. • **Sistema cerrado**—Se ha cerrado el endpoint. Gravedad baja. • **Acceso DEP no asignado**—Un salto del puntero de instrucciones a una localización no asignada en la memoria. Suele deberse a un error de aplicación, pero también podría indicar un intento (fallido) de exploit. Gravedad media. • **Ha fallado el inicio del servicio de información nativo**—Ha fallado el inicio del servicio de información. Gravedad alta.
Hora	La fecha y hora de envío de la notificación.

Monitorizado de notificaciones del servidor

- Ver notificaciones acerca del servidor ESM
- Ver detalles acerca de los logs de servidor ESM

Ver notificaciones acerca del servidor ESM

Ver notificaciones acerca del servidor ESM	
Paso 1	En la consola ESM, seleccione **Monitorizar > Logs de ESM**.
Paso 2	Para visualizar las entradas de la tabla, utilice los controles de paginado de la parte superior derecha de cada página para ver diferentes partes de la tabla.
Paso 3	(Opcional) Para ordenar las entradas de las tablas, seleccionado el encabezado de la columna para aplicar un orden ascendente. Seleccione el encabezado de la columna de nuevo para aplicar un orden descendente.
Paso 4	(Opcional) Para filtrar las entradas de la tabla, haga clic en el icono del filtro a la derecha de la columna para especificar hasta dos conjuntos de criterios para la filtración de los resultados.
Paso 5	(Opcional) Para exportar los logs a un archivo CSV, haga clic en el icono de menú y, a continuación, seleccione **Exportar logs**.

Ver detalles acerca de los logs de servidor ESM

La página **Logs de ESM** muestra notificaciones acerca del servidor ESM, incluidos fallos en la carga de archivos y acciones iniciadas desde el servidor ESM. La tabla siguiente describe los campos mostrados en la página **Monitorizar > Logs de ESM**.

Campo	Descripción
ID	Una ID numérica única para el mensaje de notificación.
Mensaje	El texto de mensaje de notificación.
Gravedad	La gravedad de la notificación, que depende del tipo de informe: • **Alta** • **Media** • **Baja**
Tipo de informe	El tipo del evento que ha activado la notificación. • **Fallo de carga de archivos** • **Protección habilitada** • **Protección deshabilitada**
Hora	La fecha y hora de envío de la notificación.

Administración de preferencias de informes y logging

Habilitar informes utilizando la consola ESM

El Endpoint Security Manager puede escribir logs en una plataforma de creación de logs externa como, por ejemplo, un sistema SIEM, servicios SOC o syslog, además de almacenar sus propios logs de forma interna. Al especificar una plataforma de creación de logs externa, es posible obtener una vista agregada de los logs de todos los servidores ESM. Puede habilitar informes externos usando la herramienta de configuración de bases de datos (DB) (consulte Habilitar informes externos usando la herramienta de configuración DB) o con el ESM. De forma predeterminada, se deshabilitan los informes externos.

Habilitar informes externos utilizando la consola ESM		
Paso 1	Vaya a la página de Informes externos.	Seleccione **Ajustes > General** y, a continuación, seleccione **Informes externos**de la lista desplegable.
Paso 2	Configure los ajustes de informes externos.	• Seleccione **verdadero** en la lista desplegable **Habilitar Syslog**. • Introduzca el nombre del host o la dirección IP del **Servidor Syslog**. • (Opcional) Introduzca el puerto de comunicación para el servidor syslog en el campo **Puerto Syslog** , un valor entre 1 y 65535 (por defecto es 514). • Seleccione **verdadero** en la lista desplegable **Habilitar log de eventos**. • (Opcional) En el campo **Agotada conexión de mensajes de mantenimiento**, introduzca un intervalo de tiempo en minutos, un valor de 0 o superior durante el que el endpoint envía un mensaje de mantenimiento al log o registro (el valor por defecto es 0). • (Opcional) En el campo **Enviar intervalo de informes**, introduzca la frecuencia de informes enviados desde el endpoint en minutos, un valor de 0 o superior (el valor por defecto es 10). Introduzca un valor de 0 si no desea recibir informes del endpoint.

Habilitar informes externos usando la herramienta de configuración DB

El ESM puede escribir logs en una plataforma de creación de logs externa; como, por ejemplo, un sistema SIEM, servicios SOC o syslog, además de almacenar sus propios logs de forma interna. Al especificar una plataforma de creación de logs externa, es posible obtener una vista agregada de los logs de todos los servidores ESM. Puede habilitar los informes externos usando el ESM (consulte Habilitar informes utilizando la consola ESM) o usando la herramienta de configuración de bases de datos (DB).

La herramienta de configuración DB es una interfaz de línea de comandos que proporciona una alternativa a la gestión de los ajustes básicos del servidor utilizando la consola EMS. Puede acceder a la herramienta de configuración DB utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. La herramienta de configuración DB se encuentra en la carpeta Servidor del servidor ESM.



Todos los comandos ejecutados utilizando la herramienta de configuración DB hacen distinción entre mayúsculas y minúsculas.

Por defecto, se deshabilitan los informes externos.

Habilitar informes externos usando la herramienta de configuración DB	
Paso 1	Abra una línea de comando como administrador: • Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**. • Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL**+**Mayús.**+**INTRO**.
Paso 2	Vaya a la carpeta que contiene la herramienta de configuración DB: `C:\Users\Administrator>`**`cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server`**

Paso 3	(Opcional) Visualice los ajustes de informes existentes:
	`C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig reporting show`**
	`EnableSyslog = True`
	`SyslogServer = CyveraServer`
	`SyslogPort = 514`
	`EnableEventLog = True`
	`KeepAliveTimeout = 0`
	`SendReportsInterval = 10`
	`MaximumReportsCount = 5000`
	`MinReportsCount = 4000`

Paso 4	Habilite los informes syslog: `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig server enablesyslog true`**
Paso 5	Introduzca la dirección IP del servidor syslog: `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig server syslogserver <ipaddress>`**
Paso 6	Especifique el puerto de comunicación para el servidor syslog, un valor entre 1 y 65535 (por defecto es 514). `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig server syslogport <portnumber>`**
Paso 7	(Opcional) Habilite el logging de eventos para enviar eventos de seguridad que Traps encuentra en el log de eventos de Windows: `C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>`**`dbconfig server enableeventlog true`**

Habilitar informes externos usando la herramienta de configuración DB (Continuación)

Paso 8 (Opcional) Introduzca un intervalo de tiempo (en minutos) durante el que el endpoint encuentra un mensaje de mantenimiento al log o informe, un valor de 0 o superior (el valor por defecto es 0):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig reporting
keepalivetimeout <value>
```

Paso 9 (Opcional) Introduzca la frecuencia de informes del endpoint en minutos, un valor de 0 o superior (el valor por defecto es 10)

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig reporting
sendreportsinterval <value>
```



Introduzca un valor de 0 si no desea recibir informes del endpoint.

Paso 10 (Opcional) Introduzca el número mínimo de notificaciones para su almacenamiento en la base de datos, un valor de 0 o superior (el valor por defecto es 5000):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig reporting
minreportscount <value>
```

Por ejemplo, la especificación de un recuento de informe mínimo de 1000 notificaciones significa que el Endpoint Security Manager retiene las 1000 notificaciones más recientes tras una limpieza de informes antiguos.

Paso 11 (Opcional) Introduzca el número máximo de notificaciones para su almacenamiento en la base de datos, un valor de 0 o superior (el valor por defecto es 4000):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig reporting
maximumreportscount <value>
```

Por ejemplo, la especificación de un recuento máximo de informes de 5000 notificaciones significa que el Endpoint Security Manager desechará las notificaciones más antiguas superiores a 5000.

Definir ajustes de comunicación usando la consola ESM

El servicio de Traps envía periódicamente mensajes al servidor Endpoint Security Manager (ESM) para informar del estado operativo del agente, informar sobre procesos que se están ejecutando en el endpoint, y para solicitar la política de seguridad más reciente. Puede cambiar la frecuencia de la comunicación entre el servidor y el endpoint usando la herramienta de configuración de bases de datos (DB) (consulte Definir ajustes de comunicación usando la herramienta de configuración DB) o usando la consola ESM.

Definir ajustes de comunicación usando la consola ESM

Paso 1	Seleccione **Configuración > General** y, a continuación, seleccione **Configuración del servidor** de la lista desplegable.
Paso 2	(Opcional) Introduzca la frecuencia (en minutos) con la que Traps envía la lista de aplicaciones que se están ejecutando en el endpoint al Endpoint Security Manager en el campo **Intervalo de inventario en minutos**.
Paso 3	(Opcional) Introduzca el periodo de gracia permitido para un dispositivo que no ha respondido (en segundos) en el campo **Periodo heartbeat en segundos** . El periodo heartbeat por defecto es de cinco minutos.

Definir ajustes de comunicación usando la herramienta de configuración DB

El servicio de Traps envía periódicamente mensajes al servidor ESM para informar del estado operativo del agente, informar sobre procesos que se están ejecutando en el endpoint, y para solicitar la política de seguridad más reciente. Puede cambiar la frecuencia de la comunicación entre el servidor y el endpoint usando el Endpoint Security Manager (consulte Definir ajustes de comunicación usando la consola ESM) o usando la herramienta de configuración de bases de datos (DB).

La herramienta de configuración DB es una interfaz de línea de comandos que proporciona una alternativa a la gestión de los ajustes básicos del servidor utilizando la consola EMS. Puede acceder a la herramienta de configuración DB utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. La herramienta de configuración DB se encuentra en la carpeta Servidor del servidor ESM.



Todos los comandos ejecutados utilizando la herramienta de configuración DB hacen distinción entre mayúsculas y minúsculas.

Definir ajustes de comunicación usando la herramienta de configuración DB

Paso 1 Abra una línea de comando como administrador:

- Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**.
- Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL**+**Mayús.**+**INTRO**.

Paso 2 Vaya a la carpeta que contiene la herramienta de configuración DB:

```
C:\Users\Administrator>cd C:\Program Files\Palo Alto Networks\Endpoint Security
Manager\Server
```

Paso 3 (Opcional) Visualice los ajustes de servidor existentes:

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig server show
PreventionsDestFolder = \\ESMServer\Quarantine
InventoryInterval = 284
HeartBeatGracePeriod = 300
NinjaModePassword = Password2
```

Paso 4 (Opcional) Introduzca el intervalo de inventario que define la frecuencia (en minutos) con la que Traps envía la lista de aplicaciones que se están ejecutando en el endpoint al Endpoint Security Manager:

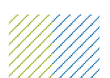
```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig server
inventoryinterval <value>
```

Si introduce un valor, por ejemplo, de 120 hace que el endpoint envíe información cada 2 horas (120 minutos).

Paso 5 (Opcional) Introduzca el periodo de gracia permitido para un dispositivo que no ha respondido (en segundos):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig server
heartbeatgraceperiod <value>
```

Si especifica un valor de 300, por ejemplo, esto significa que después de cinco minutos (300 segundos) durante el que el servidor ESM no recibe comunicación del endpoint, el Endpoint Security Manager informa del estado del endpoint como desconectado.



Solución de problemas

- ▲ Recursos para la solución de problemas de la protección avanzada del endpoint
- ▲ Herramienta de configuración de bases de datos
- ▲ Cytool
- ▲ Solución de problemas de Traps
- ▲ Solución de problemas de la consola ESM

Recursos para la solución de problemas de la protección avanzada del endpoint

Para la solución de problemas de los componentes de la Protección avanzada del endpoint, incluidos Traps y el Endpoint Security Manager, utilice los siguientes recursos.

Recurso	Descripción
Endpoint Security Manager	Interfaz web, que proporciona informes y logs. La información es útil para el monitorizado y la filtración de logs e interpretar conductas inusuales en su red. Tras analizar un evento de seguridad, puede crear una regla personalizada para el endpoint o proceso.
Log DebugWeb	Indica información, advertencias y errores relacionados con el Endpoint Security Manager. El log DebugWeb se encuentra en la carpeta %ProgramData%\Cyvera\Logs del servidor ESM.
Log de servidor	Indica información, advertencias y errores relacionados con la base de datos de endpoints y el servidor ESM. El log de servidor se encuentra en la carpeta %ProgramData%\Cyvera\Logs del servidor ESM.
Log de servicio	Indica información, advertencias y errores relacionados con el servicio de Traps. El log de servicio se encuentra en la carpeta siguiente en el endpoint: • Windows Vista y posterior: %ProgramData%\Cyvera\Logs • Windows XP: C:\Document and Settings\All Users\Application Data\Cyvera\Logs
Log de consola	Indica información, advertencias y errores relacionados con la consola de Traps. El log de consola se encuentra en la carpeta siguiente en el endpoint: • Windows Vista y posterior: C:\Users\<username>\AppData\Roaming\Cyvera • Windows XP: C:\Document and Settings\<username>\Application Data\Cyvera\Logs
Herramienta de configuración de bases de datos (DB) (dbconfig.exe)	La interfaz de líneas de comando proporciona una alternativa a la gestión de los ajustes básicos del servidor utilizando la consola EMS. Puede acceder a la herramienta de configuración DB utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. Para obtener más información, consulte Herramienta de configuración de bases de datos.
Herramienta de líneas de comando de supervisor (cytool.exe)	Le permite enumerar procesos protegidos, habilitar o deshabilitar características de protección, y habilitar o deshabilitar acciones de administración de Traps de una interfaz de líneas de comando. Para obtener más información, consulte Cytool.

Herramienta de configuración de bases de datos

La herramienta de configuración DB es una interfaz de línea de comandos que proporciona una alternativa a la gestión de los ajustes básicos del servidor utilizando la consola EMS. Puede acceder a la herramienta de configuración DB utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. La herramienta de configuración DB se encuentra en la carpeta Servidor del Endpoint Security Manager (ESM).

Utilice la herramienta de configuración DB para realizar las funciones siguientes:

- Acceso a la herramienta de configuración de bases de datos
- Administración de las licencias de Endpoint Security Manager usando la herramienta de configuración DB
- Configuración de acceso administrativo al Endpoint Security Manager utilizando la herramienta de configuración DB
- Cambio de la contraseña de modo ninja utilizando la herramienta de configuración DB
- Definir ajustes de comunicación usando la herramienta de configuración DB
- Habilitar informes externos usando la herramienta de configuración DB

Acceso a la herramienta de configuración de bases de datos

Ejecute la herramienta de configuración DB de la carpeta Servidor en un servidor ESM para ver la sintaxis y ejemplos de uso.



Todos los comandos ejecutados utilizando la herramienta de configuración DB hacen distinción entre mayúsculas y minúsculas.

Acceso a la herramienta de configuración de bases de datos	
Paso 1	Abra una línea de comando como administrador: • Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**. • Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL+Mayús.+INTRO**.
Paso 2	Vaya a la carpeta que contiene la herramienta de configuración DB: `C:\Users\Administrator>`**`cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server`**

Acceso a la herramienta de configuración de bases de datos	
Paso 3	Vea el uso y opciones para la herramienta de configuración DB:

```
c:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig

Uso:

   > DBConfig.exe importLicense [1]

       Añade una nueva licencia a la base de datos.

       1) CyveraLicense.xml ruta completa

   > DBConfig.exe [1] [2] [3]

       Escribe una configuración para la base de datos.

       1) Tipo de configuración (Servidor, Reflector, UserManagement, Información)

       2) Nombre clave

       3) Valor

   > DBConfig.exe [1] mostrar

       Muestra los valores de una configuración específica.

       1) Tipo de configuración (Servidor, Reflector, UserManagement, Información)

 Ejemplos:

> DBConfig.exe importLicense c:\Foldername\CyveraLicense.xml

> DBConfig.exe server inventoryinterval 200

> DBConfig.exe muestra el servidor
```

Cytool

Cytool es una interfaz de líneas de comando que se integra en Traps y le permite consultar y administrar funciones básicas de Traps. Los cambios realizados usando Cytool se activan hasta que Traps recibe la siguiente comunicación heartbeat del servidor ESM.

Puede acceder a la herramienta Cytool utilizando una línea de comandos de Microsoft MS-DOS ejecutado como administrador. Cytool se encuentra en la carpeta Traps en el endpoint:

Utilice Cytool para realizar las funciones siguientes:

- Acceso a Cytool
- Ver procesos actualmente protegidos por Traps
- Administración de los ajustes de protección en el endpoint
- Administración de controladores Traps y servicios en el endpoint
- Ver y comparar las políticas de seguridad en un endpoint

Acceso a Cytool

Para ver la sintaxis y ejemplos de uso para los comandos Cytool, utilice la opción `/?` después de cualquier comando.

Acceso a Cytool	
Paso 1	Abra una línea de comando como administrador: • Seleccione **Inicio > Todos los programas > Accesorios**. Haga clic con el botón derecho en **Línea de comandos**, y seleccione **Ejecutar como administrador**. • Seleccione **Inicio**. En la casilla **Iniciar búsqueda**, escriba **cmd**. A continuación, para abrir la línea de comando como administrador, pulse **CTRL**+**Mayús.**+**INTRO**.
Paso 2	Vaya a la carpeta que contiene Cytool: `C:\Users\Administrator>`**`cd C:\Program Files\Palo Alto Networks\Traps`**

Acceso a Cytool	
Paso 3	Vea el uso y opciones del comando Cytool:

```
c:\Program Files\Palo Alto Networks\Traps>cytool /?

Herramienta Traps (R) supervisor 3.1

(c) Palo Alto Networks, Inc. Todos los derechos reservados.


Uso: CYTOOL [/?] [/a] [comando [opciones]]


Opciones:

    /?             Mostrar este mensaje de ayuda.

    /a             Autenticar como supervisor.

    comando        enum | proteger | iniciar | tiempo ejecución | política


Para más información sobre la ejecución de un comando específico

    Comando CYTOOL /?
```

Ver procesos actualmente protegidos por Traps

Para ver procesos que están siendo protegidos por Traps, utilice el comando `enum` en Cytool o visualice la pestaña Protección en la consola de Traps (consulte Ver procesos actualmente protegidos por Traps). Por defecto, la consola de Traps y Cytool muestran solo los procesos protegidos iniciados por el usuario actual. Para ver los procesos protegidos iniciados por todos los usuarios, especifique la opción `/a`.

La visualización de procesos protegidos iniciados por todos los usuarios requiere la introducción de la contraseña de supervisor (desinstalación).

Ver procesos actualmente protegidos por Traps	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).
Paso 2	Vea los procesos protegidos iniciados por el usuario actual introduciendo el comando `cytool enum`. Para ver procesos protegidos para todos los usuarios del endpoint, especifique la opción `/a` e introduzca la contraseña de supervisor, cuando así se le pida.

```
c:\Program Files\Palo Alto Networks\Traps>cytool /a enum
Introducir contraseña de supervisor:
ID de proceso      Versión de agente
1000            3.1.1546
1468            3.1.1546
452             3.1.1546
[...]
```

Administración de los ajustes de protección en el endpoint

Por defecto, Traps aplica protección a los procesos clave, claves de registro, archivos de Traps, y servicios de Traps según las reglas de protección de servicio definidas en la política de seguridad (para información acerca de la configuración de reglas de protección de servicios en el Endpoint Security Manager, consulte Gestión de protección de servicios). Puede usar Cytool para cancelar las reglas de seguridad y administrar las capas siguientes de protección que Traps aplica en el endpoint:

- ▲ Habilitación o deshabilitación de protección de procesos clave en el endpoint
- ▲ Habilitación o deshabilitación de ajustes de protección de registro en el endpoint
- ▲ Habilitación o deshabilitación de ajustes de protección de Traps en el endpoint
- ▲ Habilitación o deshabilitación de ajustes de protección de servicio en el endpoint
- ▲ Uso de la política de seguridad para la administración de protección de servicios

Habilitación o deshabilitación de protección de procesos clave en el endpoint

Por defecto, Traps protege procesos clave, incluidos Cyserver.exe y CyveraService.exe basándose en las reglas de protección de servicio definidas en la política de seguridad local. Si es necesario, puede cancelar la conducta de protección de procesos clave utilizando el comando `cytool protect [enable|disable] process`.

El cambio de los ajustes de protección requiere el acceso del supervisor (desinstalar contraseña).

Habilitación o deshabilitación de ajustes de protección de procesos clave en el endpoint	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2	Para gestionar los ajustes de protección de procesos clave en el endpoint, utilice el comando siguiente:
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool protect [enable|disable] process`**
	El ejemplo siguiente muestra el resultado de la habilitación de protección de procesos clave. La columna `Modo` muestra el estado de protección revisado, `Habilitado` o `Deshabilitado`, o `Política` cuando se utilizan los ajustes de la política de seguridad local para proteger los procesos clave.
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool protect enable process`**
	`Introducir contraseña de supervisor:`
	
	`Protección      Modo        Estado`
	`Proceso         Habilitado  Habilitado`
	`Registro        Política    Deshabilitado`
	`Archivo         Política    Deshabilitado`
	`Servicio        Política    Deshabilitado`
	
	Para usar los ajustes de reglas de políticas por defecto y proteger procesos clave en el endpoint, consulte Uso de la política de seguridad para la administración de protección de servicios.

Habilitación o deshabilitación de ajustes de protección de registro en el endpoint

Para evitar que los atacantes alteren las claves de registro de Traps, utilice el comando `cytool protect enable registry` para restringir el acceso a las claves de registro guardadas en HKLM\SYSTEM\Cyvera. Para deshabilitar la protección de las claves de registro, utilice el comando `cytool protect disable registry`.

La realización de cambios en los ajustes de protección del registro requiere la introducción de la contraseña del supervisor cuando se le pida.

Habilitación o deshabilitación de ajustes de protección de registro en el endpoint	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2	Para gestionar los ajustes de protección de claves de registro en el endpoint, utilice el comando siguiente:
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool protect [enable|disable] registry`**
	El ejemplo siguiente muestra el resultado de la habilitación de protección de claves de registro. La columna `Modo` muestra el estado de protección revisado, `Habilitado` o `Deshabilitado`, o `Política` cuando se utilizan los ajustes de la política de seguridad local para proteger las claves de registro.
	`C:\Program Files\Palo Alto Networks\Traps>cytool protect enable registry`
	`Introducir contraseña de supervisor:`
	`Protección      Modo       Estado`
	`Proceso         Política   Deshabilitado`
	`Registro        Habilitado Habilitado`
	`Archivo         Política   Deshabilitado`
	`Servicio        Política   Deshabilitado`
	Para utilizar los ajustes de la política de seguridad local y proteger las claves de registro en el endpoint, consulte Uso de la política de seguridad para la administración de protección de servicios.

Habilitación o deshabilitación de ajustes de protección de Traps en el endpoint

Para evitar que los atacantes alteren los archivos de Traps, utilice el comando `cytool protect enable file` para restringir el acceso a los archivos de sistema en %Program Files%\Palo Alto Networks\Traps y %ProgramData%\Cyvera. Para deshabilitar la protección de archivos Traps, utilice el comando `cytool protect disable file`.

La realización de cambios en los ajustes de protección de archivos de Traps requiere la introducción de la contraseña del supervisor cuando se le pida.

Habilitación o deshabilitación de ajustes de protección de Traps en el endpoint	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Habilitación o deshabilitación de ajustes de protección de Traps en el endpoint (Continuación)	

Paso 2	Para gestionar los ajustes de protección de archivos de Traps en el endpoint, utilice el comando siguiente:
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool protect [enable|disable] file`**
	El ejemplo siguiente muestra el resultado de la habilitación de la protección de archivos. La columna `Modo` muestra el estado de protección revisado, `Habilitado` o `Deshabilitado`, o `Política` cuando se utilizan los ajustes de la política de seguridad local para proteger los archivos de Traps.
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool protect enable file`**
	`Introducir contraseña de supervisor:`
	
	`Protección Modo        Estado`
	`Proceso    Política    Deshabilitado`
	`Registro   Política    Deshabilitado`
	`Archivo    Habilitado  Habilitado`
	`Servicio   Política    Deshabilitado`
	
	Para usar los ajustes de reglas de políticas por defecto y proteger los archivos de Traps en el endpoint, consulte Uso de la política de seguridad para la administración de protección de servicios.

Habilitación o deshabilitación de ajustes de protección de servicio en el endpoint

Para esquivar la política de seguridad de Traps, los atacantes pueden intentar deshabilitar o cambiar el estado de los servicios de Traps. Utilice el comando `cytool protect enable service` para proteger los servicios de Traps. Para deshabilitar la protección de servicios de Traps, utilice el comando `cytool protect disable service`.

La realización de cambios en los ajustes de protección del servicio requiere la introducción de la contraseña del supervisor cuando se le pida.

Habilitación o deshabilitación de ajustes de protección de servicio en el endpoint	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Habilitación o deshabilitación de ajustes de protección de servicio en el endpoint (Continuación)

Paso 2 Para gestionar los ajustes de protección de servicios de Traps en el endpoint, utilice el comando siguiente:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect [enable|disable] service
```

El ejemplo siguiente muestra el resultado de la habilitación de protección de servicios. La columna `Modo` muestra el estado de protección revisado, `Habilitado` o `Deshabilitado`, o `Política` cuando se utilizan los ajustes de la política de seguridad local para proteger los servicios de Traps.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect enable service

Introducir contraseña de supervisor:


Protección         Modo        Estado

Proceso            Política    Deshabilitado

Registro           Política    Deshabilitado

Archivo            Política    Deshabilitado

Servicio           Habilitado  Habilitado
```

Para usar los ajustes de reglas de políticas por defecto y proteger los servicios de Traps en el endpoint, consulte Uso de la política de seguridad para la administración de protección de servicios.

Uso de la política de seguridad para la administración de protección de servicios

Tras cambiar los ajustes de protección utilizando Cytool, puede restaurar la política de seguridad por defecto en cualquier momento utilizando el comando `cytool protect policy <feature>`.

Uso de la política de seguridad para la administración de protección de servicios

Paso 1 Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2 Para usar las reglas de la política de seguridad y administrar la protección de servicios, utilice el comando siguiente:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect policy <feature>
```

donde `<feature>` es `proceso`, `registro`, `archivo`, o `servicio`.

El ejemplo siguiente muestra el resultado de la administración de la protección en los archivos de Traps utilizando la política de seguridad local. La columna `Modo` muestra el estado de protección revisado como `Política`.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect policy file
Introducir contraseña de supervisor:

Protección         Modo       Estado
Proceso            Habilitado Habilitado
Registro           Habilitado Habilitado
Archivo            Política   Deshabilitado
Servicio           Habilitado Habilitado
```

Administración de controladores Traps y servicios en el endpoint

Cuando se inicia un endpoint, Traps inicia controladores (Cyverak, Cyvrmtgn y Cyvrfsfd) y servicios (Cyvera y CyveraService) por defecto. Puede usar Cytool para cancelar la conducta por defecto y administrar el inicio o estado actual de controladores y servicios sobre una base global o individual. Los cambios en la conducta de inicio por defecto se realizan cuando se reinicia el endpoint. Los cambios en la conducta de tiempo de ejecución tienen un efecto inmediato.

- Ver componentes de inicio de Traps en el endpoint
- Habitación o deshabilitación del inicio de los componentes de Traps en el endpoint
- Ver componentes de tiempo de ejecución de Traps en el endpoint
- Inicio o parada de los componentes de tiempo de ejecución de Traps en el endpoint

Ver componentes de inicio de Traps en el endpoint

Utilice el comando `cytool startup query` para visualizar el estado de los componentes de inicio en el endpoint. Cuando se deshabilita un servicio o controlador, Cytool muestra el componente como Deshabilitado. Cuando se habilita un controlador, Cytool muestra el componente como `Sistema`. Cuando se habilita un servicio, Cytool muestra el componente `Inicio` como `Automático`.

Ver componentes de inicio de Traps en el endpoint

Paso 1 Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2 Para ver la conducta de inicio actual de controladores y servicios de Traps, utilice el comando siguiente:

```
C:\Program Files\Palo Alto Networks\Traps>cytool startup query
Servicio        Inicio
cyverak         Sistema
cyvrmtgn        Sistema
cyvrfsfd        Sistema
cyserver        Automático
CyveraService   Automático
```

Habitación o deshabilitación del inicio de los componentes de Traps en el endpoint

Use el comando `cytool startup [enable|disable]` seguido opcionalmente por el nombre del componente para cancelar la conducta por defecto e iniciar los controladores y servicios de Traps en el endpoint.

La realización de cambios en la conducta de inicio requiere la introducción de la contraseña del supervisor cuando se le pida.



Los cambios en los controladores y servicios de Traps no se hacen efectivos hasta el reinicio del sistema. Para hacer que los cambios en los controladores y servicios de Traps surtan efecto inmediatamente, consulteInicio o parada de los componentes de tiempo de ejecución de Traps en el endpoint.

Habilitación o deshabilitación del inicio de los componentes de Traps en el endpoint	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2	Para cambiar la conducta de inicio para un controlador o servicio específicos, utilice el comando siguiente:
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool startup [enable|disable] <component>`**
	donde `<component>` es un controlador: `cyverak`, `cyvrmtgn`, `cyvrfsfd`; o un servicio: `cyserver`, `CyveraService`.
	Alternativamente, puede omitir `<component>` del comando para cambiar la conducta de inicio para todos los controladores y servicios.
	El ejemplo siguiente muestra el resultado para la deshabilitación de la conducta de inicio del controlador cyvrmtgn. La columna **`Inicio`** muestra la conducta revisada como `Deshabilitada`.
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool startup disable cyvrmtgn`**
	`Introducir contraseña de supervisor:`
	
	`Servicio          Inicio`
	`cyverak           Sistema`
	`cyvrmtgn          Deshabilitado`
	`cyvrfsfd          Sistema`
	`cyserver          Automático`
	`CyveraService     Automático`

Ver componentes de tiempo de ejecución de Traps en el endpoint

Utilice el comando `cytool runtime query` para visualizar el estado de los componentes de Traps en el endpoint. Cuando un servicio o controlador está activo, Cytool muestra el componente como `En ejecución`. Cuando no se está ejecutando un servicio o controlador, Cytool muestra el componente como `Detenido`.

Ver componentes de inicio de Traps en el endpoint	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2	Para ver el estado de tiempo de ejecución actual de controladores y servicios de Traps, utilice el comando siguiente:
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool runtime query`**
	`Servicio          Estado`
	`cyverak           En ejecución`
	`cyvrmtgn          En ejecución`
	`cyvrfsfd          En ejecución`
	`cyserver          En ejecución`
	`CyveraService     Detenido`

Inicio o parada de los componentes de tiempo de ejecución de Traps en el endpoint

En situaciones en las que no tiene permiso para cambiar la conducta de Traps desde el Endpoint Security Manager pero debe solucionar un problema urgente relacionado con los controladores y servicios Traps, puede usar el comando `cytool startup [enable|disable]` para cancelar la conducta del tiempo de ejecución por defecto. El comando es útil cuando se debe tomar una acción inmediata para iniciar o detener todos los componentes de Traps o iniciar o detener un controlador o servicio específico de Traps.



Los cambios en la conducta de tiempo de ejecución de controladores y servicios de Traps se ponen a cero cuando se reinicia el sistema. Para realizar cambios en la conducta de inicio de controladores y servicios de Traps, consulteHabitación o deshabilitación del inicio de los componentes de Traps en el endpoint.

La realización de cambios en la conducta de tiempo de ejecución requiere la introducción de la contraseña del supervisor cuando se le pida.

Inicio o parada de los componentes de tiempo de ejecución de Traps en el endpoint	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2	Para iniciar o detener un controlador o servicio, utilice el comando siguiente:
	`C:\Program Files\Palo Alto Networks\Traps>`**`cytool runtime start <component>`**
	donde `<component>` es un controlador: `cyverak`, `cyvrmtgn`, `cyvrfsfd`; o un servicio: `cyserver`, `CyveraService`.
	Alternativamente, puede omitir `<component>` del comando para cambiar la conducta de tiempo de ejecución para todos los controladores y servicios.
	El ejemplo siguiente muestra el resultado cuando se para el servicio `cyserver`. La columna `Inicio` muestra el estado de los componentes revisados, `En ejecución` o `Parado`.
	`C:\Program Files\Palo Alto Networks\Traps>cytool runtime stop cyserver`
	`Introducir contraseña de supervisor:`
	
	`Servicio      Inicio`
	`cyverak       En ejecución`
	`cyvrmtgn      En ejecución`
	`cyvrfsfd      En ejecución`
	`cyserver      Parado`
	`CyveraService En ejecución`

Ver y comparar las políticas de seguridad en un endpoint

Usando Cytool, puede mostrar detalles acerca de políticas de seguridad en el endpoint.

- ▲ Ver detalles acerca de una política activa
- ▲ Comparar políticas

Ver detalles acerca de una política activa

Use el comando `cytool policy query <process>` para ver detalles acerca de políticas asociadas con un proceso específico. El resultado es de utilidad cuando se desea verificar que se implementa una política en el modo previsto.

Para ver los detalles de la política, debe introducir la contraseña del supervisor, cuando así se solicita.

Ver detalles acerca de una política activa	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Paso 2	Para ver la política activa para un proceso, use el siguiente comando:
	`C:\Program Files\Palo Alto Networks\Traps>cytool policy query <process>`
	donde `<process>` es el nombre de proceso o la ID de proceso (PID). Por ejemplo, para ver detalles acerca de una política para el bloc de notas, introduzca `cytool policy query notepad`. El ejemplo siguiente muestra detalles de las políticas para un proceso con PID 1234.
	`C:\Program Files\Palo Alto Networks\Traps>cytool policy query 1234`
	`Introducir contraseña de supervisor:`
	
	`Genérico`
	`  Habilitar                      0x00000001`
	`  SuspendOnce                    0x00000001`
	`  AdvancedHooks                  0x00000001`
	
	`[...]`

Comparar políticas

En intervalos regulares, Traps solicita una política de seguridad actualizada del Endpoint Security Manager y la guarda en el registro del sistema. Cuando un usuario inicia un proceso, Traps determina si protege o no el proceso según los ajustes de la política de seguridad.

En escenarios de solución de problemas en los que Traps no se comporta según lo previsto, utilice el comando `cytool policy compare` para ver las diferencias en políticas que se aplican a procesos que se ejecutan en el endpoint. Utilizando el comando, puede comparar una política para un proceso con la política de seguridad por defecto o comparar una política para un proceso con una política para otro proceso. En ambos casos, puede especificar el nombre del proceso o la ID del proceso (DIP). La especificación del nombre del proceso simula la aplicación de la política para el proceso. Al especificar el PID se consulta la política efectiva para el proceso en ejecución. Cytool muestra los ajustes de políticas punto por punto e indica cualquier diferencia entre los políticas en rojo.

Para comparar políticas, debe introducir la contraseña del supervisor, cuando así se solicita.

Comparar políticas	
Paso 1	Abra una línea de comandos como administrador y vaya a la carpeta Traps (consulte Acceso a Cytool).

Comparar políticas (Continuación)

Paso 2 Compare los detalles de dos políticas:

- Para comparar la política con la política por defecto, utilice el comando siguiente:

  `C:\Program Files\Palo Alto Networks\Traps>`**`cytool policy compare <process> default`**

  donde `<process>` es el nombre de proceso o la ID de proceso (PID).

  El ejemplo siguiente muestra el resultado de la comparación de una política que se aplica al bloc de notas con la política por defecto. Las diferencias entre las dos políticas se muestran en rojo.

```
C:\Program Files\Palo Alto Networks\Traps>cytool policy compare notepad default
Introducir contraseña de supervisor:

Genérico
  Habilitar                              0x00000001                    0x00000001
  SuspendOnce                            0x00000001                    0x00000001
  AdvancedHooks                          0x00000001                    0x00000001

[...]

DllSec
  Habilitar                              0x00000001                    0x00000000
  Optimizar                              0x00000001                    0x000000011

[...]
```

- Para comparar las políticas para dos procesos, utilice el comando siguiente:

  `C:\Program Files\Palo Alto Networks\Traps>`**`cytool policy compare <process1> <process2>`**

  donde `<process1>` y `<process2>` son el nombre del proceso o ID del proceso (PID). Por ejemplo, para comparar la política aplicada a iexplorer con la política aplicada a chrome, introduzca `cytool policy compare iexplorer chrome`. También puede comparar las políticas para dos PID o comparar la política de un proceso con una política de un PID.

  El ejemplo siguiente muestra el resultado de la comparación de las políticas aplicadas a dos PID, 1592 y 1000. Las diferencias entre las dos políticas se muestra en rojo.

```
C:\Program Files\Palo Alto Networks\Traps>cytool policy compare 1592 1000
Introducir contraseña de supervisor:

Genérico
  Habilitar                              0x00000001                    0x00000001
  SuspendOnce                            0x00000001                    0x00000001
  AdvancedHooks                          0x00000001                    0x00000001

[...]

DllSec
  Habilitar                              0x00000001                    0x00000000
  Optimizar                              0x00000001                    0x000000011

[...]
```

Solución de problemas de Traps

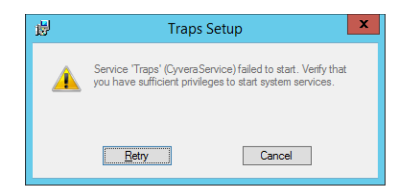
Este tema está dirigido a los siguientes problemas relacionados con Traps:

- ¿Por qué no puedo instalar Traps?
- ¿Por qué no puedo actualizar o desinstalar Traps?
- ¿Por qué no se puede conectar Traps con el servidor ESM?
- ¿Cómo soluciono un error de certificado de servidor de Traps?

¿Por qué no puedo instalar Traps?

Síntoma

Configuración de Traps informa del error siguiente: No se ha podido iniciar el servicio “Traps” (CyveraService). Verifique que tiene los privilegios suficientes.



Causas posibles

- No tiene privilegios administrativos para iniciar servicios en el endpoint.

Solución

Después de cada paso del procedimiento siguiente, verifique si puede instalar Traps. Si Traps sigue informando de un error, proceda con cada paso posterior hasta solucionar el problema.

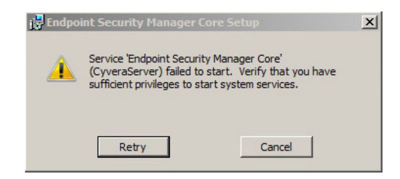
Solución: ¿Por qué no puedo instalar Traps?	
Paso 1	Verifique que tiene derechos administrativos en el endpoint: • Windows 7: Haga clic en **Inicio > Panel de control > Cuentas de usuario > Administrar cuentas de usuario**. En la pestaña de usuario, verifique que su nombre de usuario está en el grupo Administradores. • Windows 8: Haga clic en **Inicio > Panel de control > Cuentas de usuario > Cambiar cuentas de usuario**. Verifique que la cuenta aparece como Administrador. Inicie sesión en el endpoint como administrador válido.

Solución: ¿Por qué no puedo instalar Traps?	
Paso 2	El archivo de log de servicio contiene información, advertencias y errores relacionados con el servicio de Traps. Para la solución adicional de un problema relacionado con el servicio de Traps, abra el archivo C:\ProgramData\Cyvera\Logs\Service.log en un editor de texto y revise cualquier error en el archivo de log que ha ocurrido en el momento del evento.  Por defecto, la carpeta Datos de programa puede estar oculta. Para ver la carpeta en Windows Explorer, seleccione **Organizar > Opciones de carpeta y búsqueda > Ver > Mostrar archivos y carpetas ocultos**.
Paso 3	Si el problema persiste, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.

¿Por qué no puedo actualizar o desinstalar Traps?

Síntoma

Configuración de Traps informa del error siguiente: No se ha podido iniciar el servicio "Traps" (CyveraService). Verifique que tiene los privilegios suficientes.



Causas posibles

En versiones anteriores de Traps, la función de protección de servicio evita la modificación o alteración de los archivos de sistema de Traps.

Solución

Solución: ¿Por qué no puedo actualizar Traps?	
Paso 1	Cree una regla de acción para deshabilitar la protección de servicio (consulte Gestión de protección de servicios).
Paso 2	Verifique que puede instalar o desinstalar Traps.
Paso 3	Borre la regla de acción (consulte Guardar reglas).
Paso 4	Intente actualizar Traps. Para la solución de un problema relacionado con el servicio de Traps, visualice los logs para ver si Traps informa de un error específico: • En la consola de Traps, seleccione **Abrir archivo de log**. • Desde la consola de Traps, seleccione **Enviar archivo de soporte** para enviar los logs al servidor ESM • Cree una regla de acción para recuperar los logs del endpoint (consulte Gestión de datos recopilados por Traps).
Paso 5	Si el problema persiste, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.

¿Por qué no se puede conectar Traps con el servidor ESM?

Síntoma

Traps no se puede comunicar con el servidor ESM para obtener la política de seguridad más reciente e informa de un estado de **¡Sin conexión con el servidor!**.

Causas posibles

- Las especificaciones del servidor o el endpoint no cumplen con los requisitos previos de instalación y criterios.
- El servicio de Traps no está activo en el endpoint.
- El servicio básico del Administrador de seguridad de endpoints no está activa en el servidor ESM.
- El endpoint no está conectado a la red.
- No se permite tráfico entrante en el puerto para el servidor ESM (por defecto es 2125).
- Se habilita el cortafuegos de Windows en el servidor ESM y evita que el servidor se comunique con el cliente.
- El certificado del endpoint no coincide con el certificado del servidor ESM (consulte ¿Cómo soluciono un error de certificado de servidor de Traps?)

Solución

Tras cada paso en el procedimiento siguiente, verifique si Traps puede conectarse con el servidor ESM seleccionando **Registrar ahora**. Si Traps no puede conectarse con el servidor, proceda con cada paso posterior hasta solucionar el problema.

Solución: ¿Por qué no se puede conectar Traps con el servidor ESM?		
Paso 1	Verifique que el servidor y endpoint cumplen los requisitos previos.	Consulte Requisitos previos.
Paso 2	Verifique que el servicio de Traps se está ejecutando en el endpoint.	1. Abra el administrador de servicios: • Windows XP: En el menú de inicio, seleccione **Panel de control > Herramientas administrativas > Servicios**. • Windows Vista y posterior: En el menú de inicio seleccione **Panel de control > Sistema y seguridad > Herramientas administrativas > Servicios**. 2. Localice el servicio de Traps (denominado CyveraService en versiones anteriores de Traps) y verifique que el estado del servicio sea **Iniciado**. 3. Si el estado del servicio es **Detenido**, haga doble clic en el servicio y seleccione **Inicio**. Haga clic en **Cerrar**.

Solución: ¿Por qué no se puede conectar Traps con el servidor ESM? (Continuación)		
Paso 3	Verifique que el servicio básico del Endpoint Security Manager se está ejecutando en el servidor ESM:	1. Abra el administrador de servicios: • Windows Server 2008: En el menú de inicio, seleccione **Panel de control > Herramientas administrativas > Servicios**. • Windows Server 2012: En el menú de inicio seleccione **Panel de control > Sistema y seguridad > Herramientas administrativas > Servicios**. 2. Localice el servicio básico del Endpoint Security Manager (denominado CyveraServer en versiones anteriores del Endpoint Security Manager) y verifique que el estado del servicio sea **Iniciado** (Windows Server 2008) o **En ejecución** (Windows Server 2012). 3. Si el estado del servicio es **Detenido** o **En pausa**, haga doble clic en el servicio y seleccione **Inicio**. Haga clic en **Cerrar**.
Paso 4	Verifique que puede llegar al servidor ESM desde el endpoint.	Desde el endpoint, abra una línea de comando y haga ping a la dirección IP o el nombre host del servidor ESM. Si no se puede acceder al servidor ESM, examine los ajustes de conectividad de red entre los dispositivos.
Paso 5	Verifique que puede llegar al endpoint desde el servidor ESM.	Desde el servidor ESM, abra una línea de comando y haga ping a la dirección IP o el nombre host del endpoint. Si no se puede acceder al endpoint, examine los ajustes de conectividad de red entre los dispositivos.
Paso 6	Verifique que el puerto para el servidor ESM está abierto en el cortafuegos de Windows (por defecto es 2125).	1. Para comprobar el acceso del puerto desde el endpoint: a. Abra una línea de comando como administrador. b. Introduzca el comando siguiente para telnet en el puerto 2125 en el servidor ESM: `C:\>telnet <esmservername> 2125` donde `<esmservername>` es el nombre de host o la dirección IP del servidor ESM. 2. Si no puede conectar a telnet en el puerto 2125, cree una regla entrante para abrir ese puerto: a. Abra los ajustes avanzados del cortafuegos de Windows: – Windows Server 2008: En el menú de inicio, seleccione **Panel de control > Cortafuegos de Windows > Ajustes avanzados**. – Windows Server 2012: En el menú de inicio, seleccione **Panel de control > Sistema y seguridad > Cortafuegos de Windows > Ajustes avanzados**. b. Seleccione **Reglas entrantes**. c. Cree una nueva regla para permitir que Traps se comunique con el Endpoint Security Manager en el puerto 2125 seleccionando el asistente de Nueva regla y siguiendo las instrucciones. 3. Verifique que puede conectarse ahora con telnet en el puerto 2125 en el servidor ESM desde el endpoint.

Solución: ¿Por qué no se puede conectar Traps con el servidor ESM? (Continuación)		
Paso 7	Deshabilite temporalmente el cortafuegos de Windows.	1. Abra los ajustes de Cambiar centro de acción: • Windows Server 2008: En el menú de inicio, seleccione **Panel de control**. Haga doble clic en **Centro de acción** y seleccione **Ajustes de Cambiar centro de acción**. • Windows Server 2012: En el menú de inicio seleccione **Panel de control > Sistema y seguridad**. Haga doble clic en **Centro de acción** y seleccione **Ajustes de Cambiar centro de acción**. 2. Deseleccione la opción **Cortafuegos de red**. 3. Haga clic en **ACEPTAR**.
Paso 8	Verifique que se recupera la conectividad entre Traps y el servidor ESM.	En la consola Traps, haga clic en **Registrar ahora**. Si se establece la conectividad, el estado de conexión aparece como **Con éxito**.
Paso 9	Vea los logs para comprobar si Traps informa de un error específico:	• En la consola de Traps, seleccione **Abrir archivo de log**. • Desde la consola de Traps, seleccione **Enviar archivo de soporte** para enviar los logs al servidor ESM • Cree una regla de acción para recuperar los logs del endpoint (consulte Gestión de datos recopilados por Traps).
Paso 10	Si el problema persiste, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.	

¿Cómo soluciono un error de certificado de servidor de Traps?

Síntoma

Aparece el siguiente error en services.log del endpoint:

"Se ha producido un error durante la solicitud HTTP a https://<hostname>:2125/CyveraServer/. Esto puede deberse al hecho de que el certificado del servidor no se configura correctamente con HTTP.SYS en el caso de HTTPS. Esto también puede deberse a una falta de coincidencia del enlace de seguridad entre el cliente y el servidor".

Causas posibles

Cuando se instala el software del servidor ESM, se dispone de los siguientes ajustes de configuración de certificados: Sin certificado (**Sin SSL**) y certificado externo (**SSL**). Para instalar Traps, debe seleccionar **SSL** si ha seleccionado Certificado externo durante la instalación del software del servidor ESM o **Sin SSL** si ha seleccionado Sin certificado. La falta de coincidencia en los ajustes causa el error del que se informa a service.log.

Solución

Solución: ¿Cómo soluciono un error de certificado de servidor de Traps?		
Paso 1	Reinstale el software Traps.	Verifique los ajustes SLL para el servidor ESM y reinstale Traps en el endpoint, teniendo cuidado de seleccionar el ajuste de SLL apropiado durante la instalación (consulte Instalación de Traps en el endpoint).
Paso 2	Verifique que el error no aparece en el log.	En la consola de Traps, seleccione **Abrir archivo de log**, o abra services.log en el endpoint y revise cualquier error reciente. Si el error de certificado de servidor persiste, póngase en contacto con el equipo de soporte de Palo Alto Networks.

Solución de problemas de la consola ESM

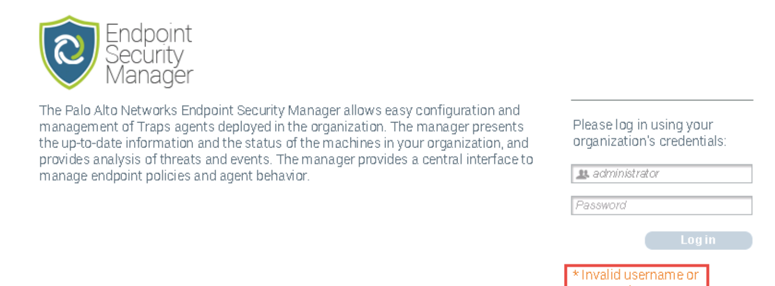
Este tema está dirigido a los siguientes problemas relacionados con la consola del Endpoint Security Manager (ESM):

- ▲ ¿Por qué no puedo iniciar sesión en la consola ESM?
- ▲ ¿Por qué recibo un error de servidor cuando inicio la consola ESM?
- ▲ ¿Por qué aparecen todos los endpoints como desconectados en la consola ESM?

¿Por qué no puedo iniciar sesión en la consola ESM?

Síntoma

La consola del Endpoint Security Manager (ESM) muestra un mensaje de error en el que se indica que el nombre de usuario o la contraseña no son válidos.





Causas posibles

- No se ha introducido correctamente el nombre de usuario o la contraseña.
- El usuario especificado durante la instalación inicial no tiene privilegios de propietario de DB.
- No se ha añadido el usuario como administrador.
- El usuario que instaló el servidor no era un administrador local en el servidor.

Solución

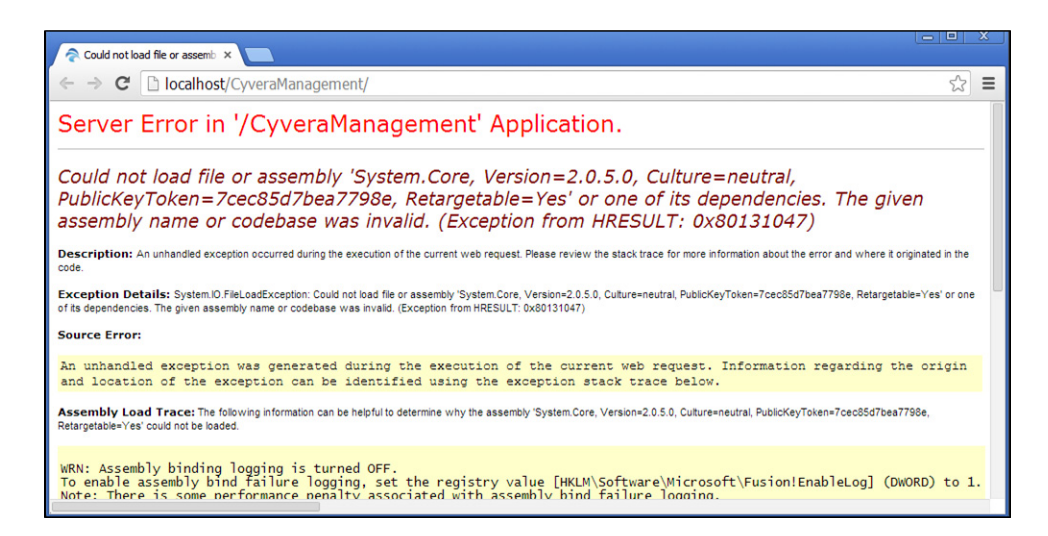
Solución: ¿Por qué no puedo iniciar sesión en la consola ESM?	
Paso 1	Verifique que ha introducido el nombre de usuario y contraseña correctos.
Paso 2	Verifique que el usuario tiene privilegios de propietario de DB (consulte Configuración de la base de datos del servidor MS-SQL).

Solución: ¿Por qué no puedo iniciar sesión en la consola ESM?	
Paso 3	Inicie sesión como administrador y verifique que el modo de autenticación sea correcto y que la cuenta de usuario aparezca en la página Administración de usuario. Para añadir un usuario administrativo, consulte Configuración de acceso administrativo al Endpoint Security Manager utilizando la consola ESM. Alternativamente, puede añadir el administrador usando la herramienta de configuración de bases de datos (consulte Configuración de acceso administrativo al Endpoint Security Manager utilizando la herramienta de configuración DB).
Paso 4	Si no puede iniciar sesión como administrador, reinstale el Endpoint Security Manager como administrador local.
Paso 5	Reinicie IIS: Haga clic en **Iniciar > Ejecutar**, tipo **Reiniciar IIS**, y haga clic en **ACEPTAR**.
Paso 6	Verifique que puede iniciar sesión en la consola del Endpoint Security Manager usando la cuenta. Si el problema persiste, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.

¿Por qué recibo un error de servidor cuando inicio la consola ESM?

Síntoma

Cuando se abre la consola del Endpoint Security Manager (ESM), se recibe un error en el navegador que indica un error de servidor en la aplicación '/CyveraManagement' or '/EndpointSecurityManager'.



Causas posibles

El servidor no cumple el requisito previo para .NET Framework 4.0 con la actualización KB2468871.

Solución

Instale .NET Framework 4.0 y el parche KB2468871.

¿Por qué aparecen todos los endpoints como desconectados en la consola ESM?

Síntoma

La página de estado de la consola del Endpoint Security Manager (ESM) informa de que todos los endpoints están desconectados, incluso cuando el endpoint puede llegar al servidor ESM.

Causas posibles

- El servidor ESM no cumple los requisitos previos.
- Debe reiniciarse el servicio básico del Administrador de seguridad de endpoints. Esto ocurre si se espera más de una hora para instalar la clave de licencia tras la instalación inicial del software de la consola ESM.
- No se permite tráfico entrante en el puerto asociado con el servidor ESM (por defecto es 2125).

Solución

Tras cada paso en el procedimiento siguiente, verifique si Traps puede conectarse con el servidor ESM seleccionando **Registrar ahora**. Si Traps no puede conectarse con el servidor, proceda con cada paso posterior hasta solucionar el problema.

Solución: ¿Por qué aparecen todos los endpoints como desconectados en la consola ESM?		
Paso 1	Verifique que el servidor cumple los requisitos previos.	Consulte Requisitos previos para la instalación del servidor ESM.
Paso 2	Verifique que el servicio de Traps se está ejecutando en el endpoint.	1. Abra el administrador de servicios: • Windows XP: En el menú de inicio, seleccione **Panel de control > Herramientas administrativas > Servicios**. • Windows Vista y posterior: En el menú de inicio seleccione **Panel de control > Sistema y seguridad > Herramientas administrativas > Servicios**. 2. Localice el servicio de Traps (denominado CyveraService en versiones anteriores de Traps) y verifique que el estado de servicio sea **Iniciado**. 3. Si el estado del servicio es **Detenido**, haga doble clic en el servicio y seleccione **Inicio**. Haga clic en **Cerrar**.

Solución: ¿Por qué aparecen todos los endpoints como desconectados en la consola ESM? (Continuación)		
Paso 3	Verifique que el servicio básico del Endpoint Security Manager se está ejecutando en el servidor ESM:	1. Abra el administrador de servicios: • Windows Server 2008: En el menú de inicio, seleccione **Panel de control > Herramientas administrativas > Servicios**. • Windows Server 2012: En el menú de inicio seleccione **Panel de control > Sistema y seguridad > Herramientas administrativas > Servicios**. 2. Localice el Endpoint Security Manager servicio básico (denominado CyveraServer en versiones anteriores del Endpoint Security Manager) y verifique que el estado del servicio **Iniciado** (Windows Server 2008) o **En ejecución** (Windows Server 2012). 3. Si el estado del servicio es **Detenido** o **En pausa**, haga doble clic en el servicio y seleccione **Inicio**. Haga clic en **Cerrar**.
Paso 4	Verifique que el puerto para el servidor ESM está abierto en el cortafuegos de Windows (por defecto es 2125).	1. Para comprobar el acceso del puerto desde el endpoint: a. Abra una línea de comando como administrador. b. Introduzca el comando siguiente para telnet en el puerto 2125 en el servidor ESM: C:\>**telnet <esmservername> 2125** donde <esmservername> es el nombre de host o la dirección IP del servidor ESM. 2. Si no puede conectar a telnet en el puerto 2125, cree una regla entrante para abrir ese puerto: a. Abra los ajustes avanzados del cortafuegos de Windows: – Windows Server 2008: En el menú de inicio, seleccione **Panel de control > Cortafuegos de Windows > Ajustes avanzados**. – Windows Server 2012: En el menú de inicio, seleccione **Panel de control > Sistema y seguridad > Cortafuegos de Windows > Ajustes avanzados**. b. Seleccione **Reglas entrantes**. c. Cree una nueva regla para permitir que Traps se comunique con el Endpoint Security Manager en el puerto 2125 seleccionando el asistente de Nueva regla y siguiendo las instrucciones. 3. Verifique que puede conectarse ahora con telnet en el puerto 2125 en el servidor ESM desde el endpoint.

Solución: ¿Por qué aparecen todos los endpoints como desconectados en la consola ESM? (Continuación)		
Paso 5	Deshabilite temporalmente el cortafuegos de Windows.	1. Abra los ajustes de Cambiar centro de acción: • Windows Server 2008: En el menú de inicio, seleccione **Panel de control**. Haga doble clic en **Centro de acción** y seleccione **Ajustes de Cambiar centro de acción**. • Windows Server 2012: En el menú de inicio seleccione **Panel de control > Sistema y seguridad**. Haga doble clic en **Centro de acción** y seleccione **Ajustes de Cambiar centro de acción**. 2. Deseleccione la opción **Cortafuegos de red**. 3. Haga clic en **ACEPTAR**.
Paso 6	Verifique que se recupera la conectividad entre Traps y el servidor ESM.	En la consola Traps, haga clic en **Registrar ahora**. Si se establece la conectividad, el estado de conexión aparece como **Con éxito**. Si el problema persiste, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.